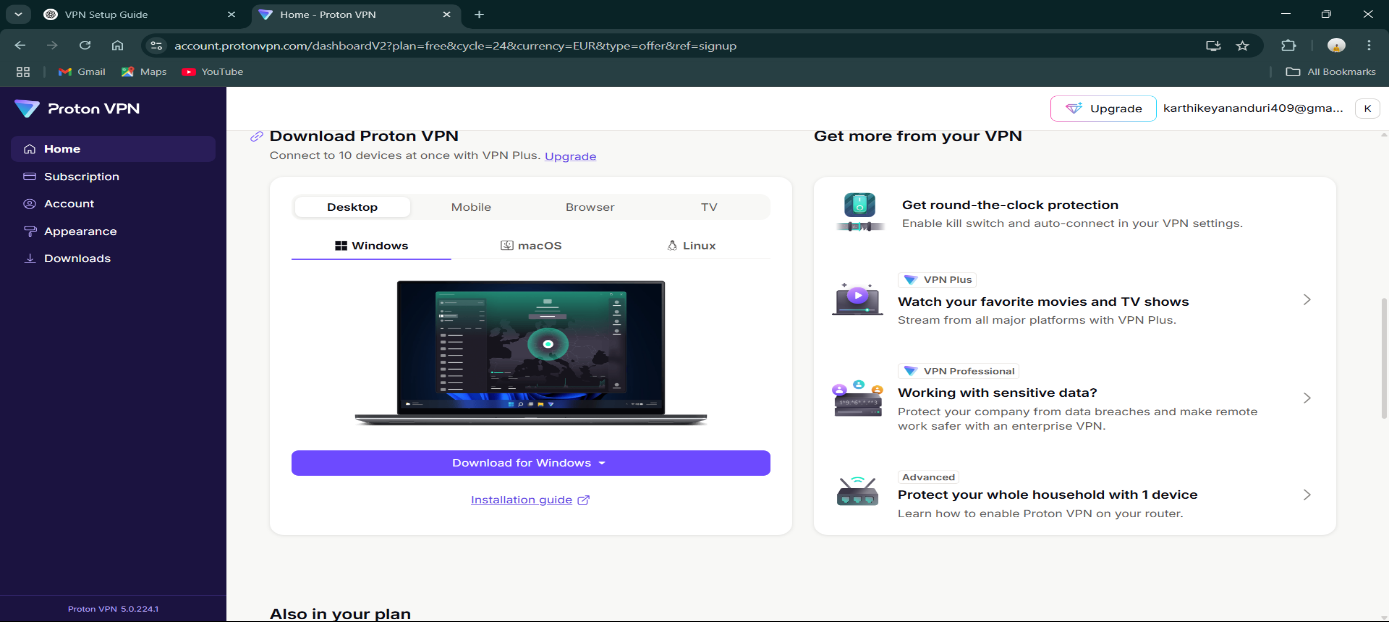
TASK – 8

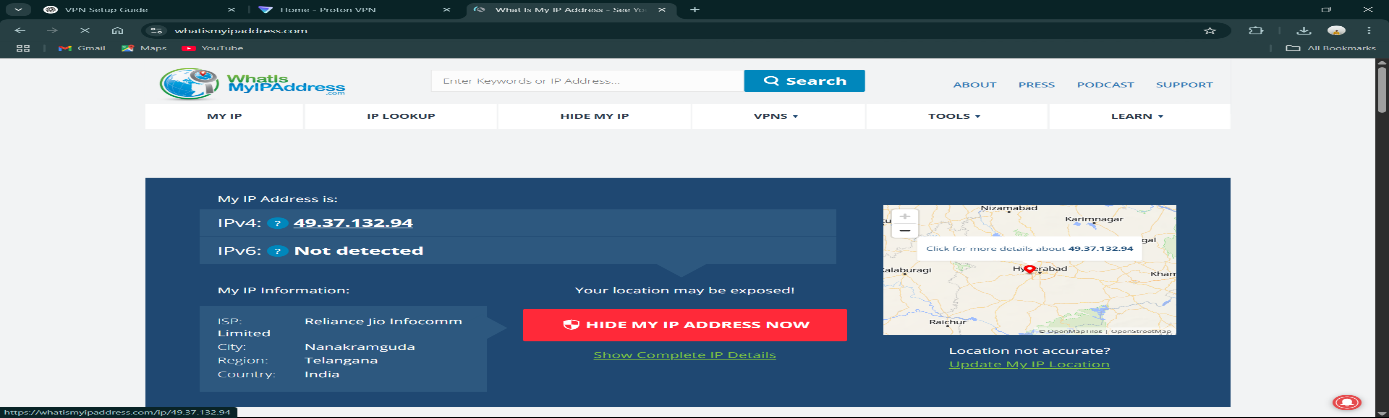
## VPNs and understanding of privacy tools.

**ProtonVPN Service Selection and Download Page**

****

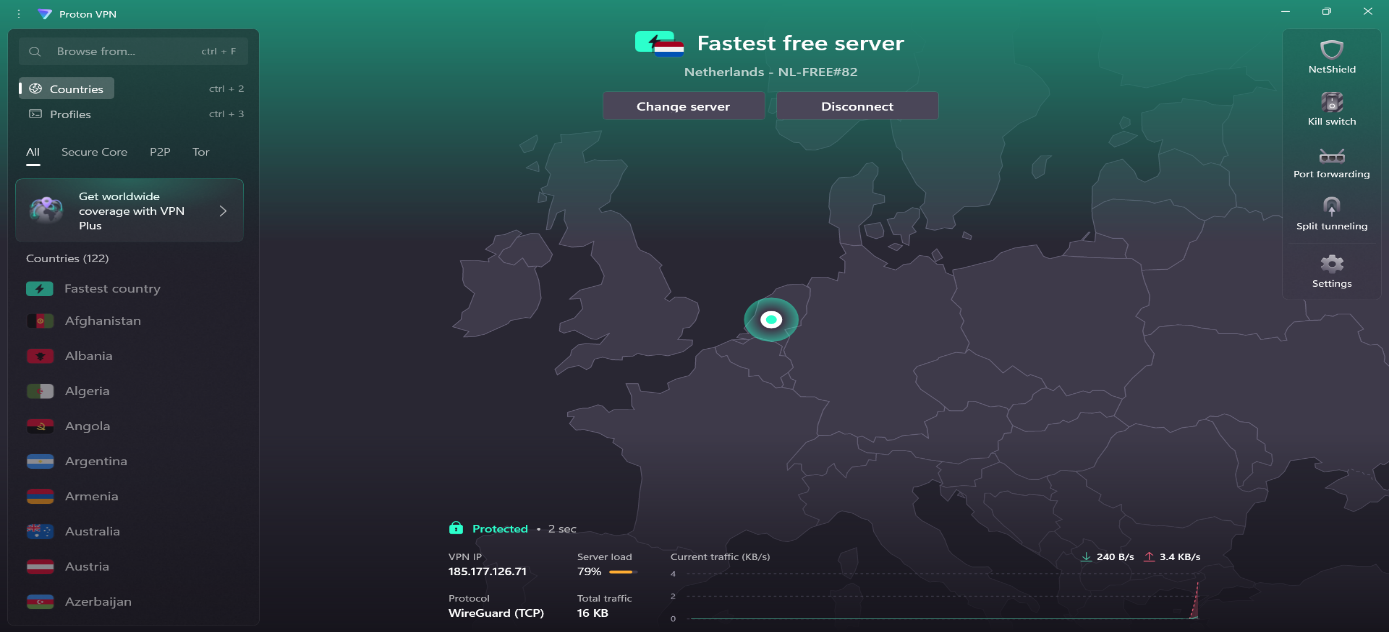
This screenshot shows the ProtonVPN download page after successful account registration. ProtonVPN was selected as the free VPN service for this project due to its strong reputation for privacy and security. The interface displays download options for different platforms (Windows, macOS, Linux) and various subscription tiers including VPN Plus features like round-the-clock protection, streaming capabilities, and enterprise solutions. The download button for Windows is prominently displayed, ready for client installation.

**Original IP Address Verification (Before VPN Connection)**

****

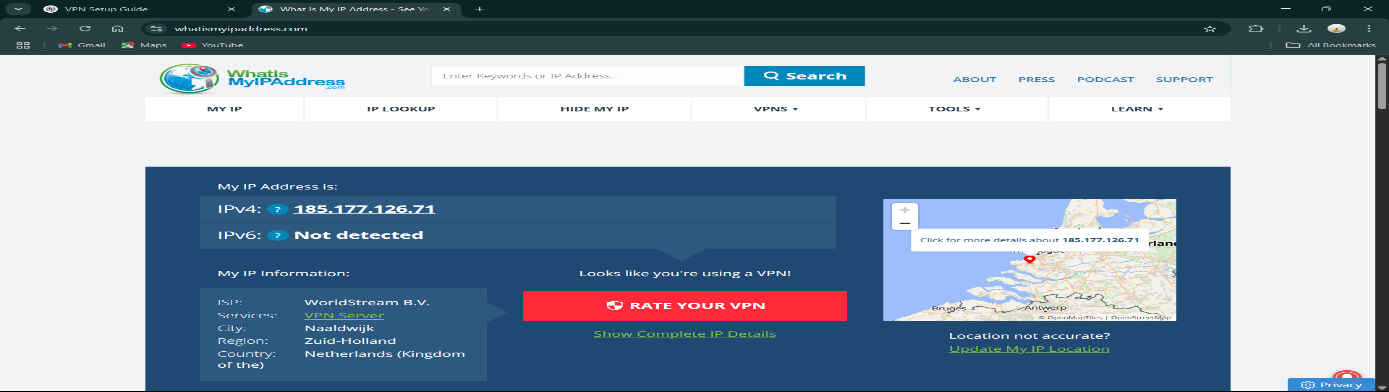
This screenshot from whatismyipaddress.com shows the original IP address and location before connecting to the VPN. The displayed IP address is 49.37.132.94, with the ISP identified as Reliance Jio Infocomm Limited. The geographic location is shown as Nanakramguda, Telangana, India, which represents the actual physical location and internet service provider. This serves as the baseline for comparing the changes after VPN connection.

**ProtonVPN Client Interface - Connected to Netherlands Server**

****

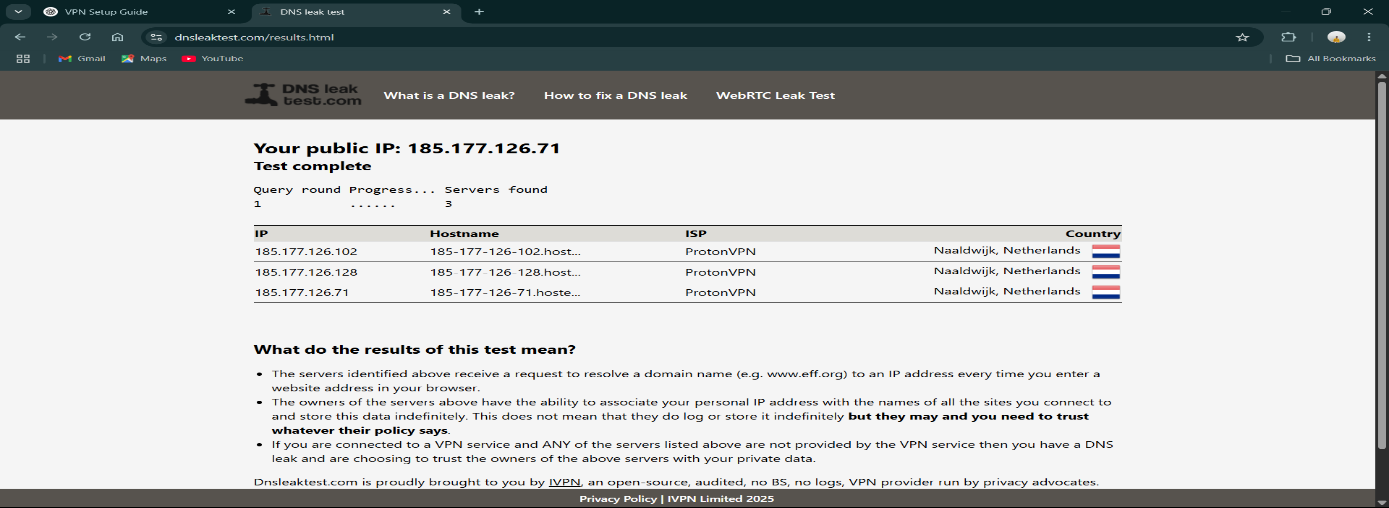
This screenshot displays the ProtonVPN client interface after successfully connecting to a server in the Netherlands (NL-FREE#82). The application shows "Protected" status with a connection time of 2 seconds. Key technical details are visible including the VPN IP address (185.177.126.71), WireGuard protocol usage, server load at 79%, and real-time traffic monitoring showing 240 B/s download and 3.4 KB/s upload speeds. The interface also shows available security features like NetShield, Kill switch, Port forwarding, and Split tunneling.

**IP Address Verification After VPN Connection**

****

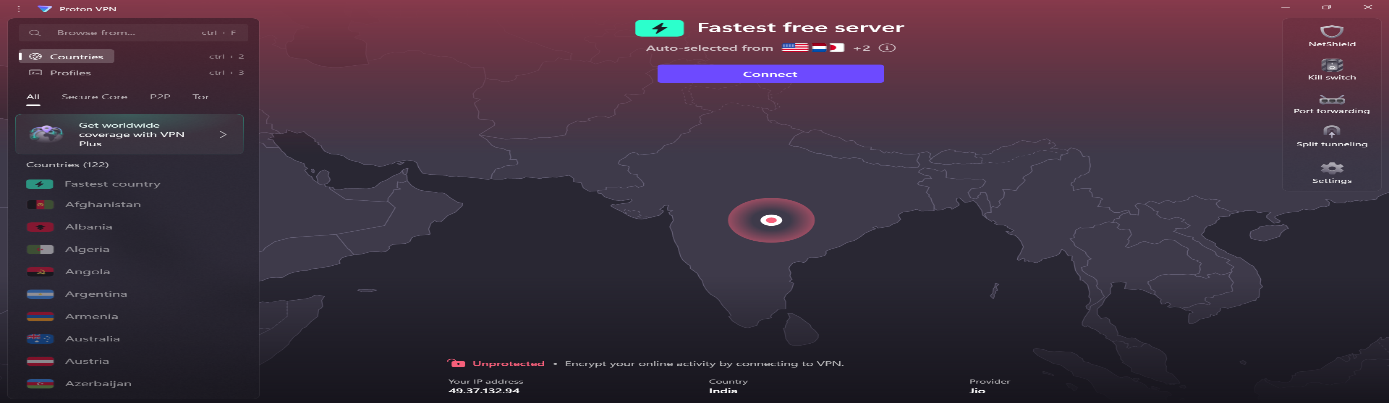
This screenshot confirms successful IP address masking through the VPN connection. The IP address has changed from the original Indian IP (49.37.132.94) to a Netherlands-based IP (185.177.126.71). The ISP is now shown as "WorldStream B.V." with the location changed to Naaldwijk, Zuid-Holland, Netherlands. The website correctly identifies VPN usage with the message "Looks like you're using a VPN!" This demonstrates the successful geographic location masking capability of the VPN service.

**DNS Leak Test Results**

****

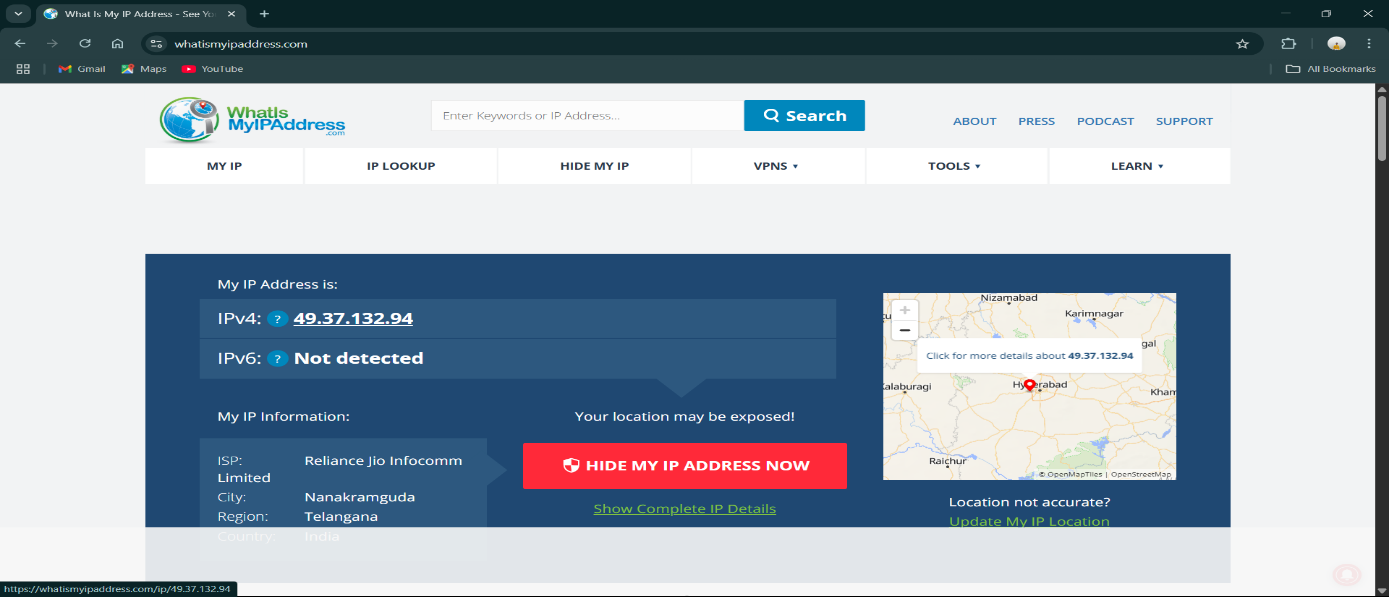
This screenshot shows the results of a DNS leak test performed while connected to the VPN. The test confirms that DNS queries are being properly routed through ProtonVPN servers, with all detected DNS servers (185.177.126.102, 185.177.126.128, 185.177.126.71) belonging to ProtonVPN and located in Naaldwijk, Netherlands. This is crucial for privacy as it ensures that DNS requests are not leaking through the original ISP, maintaining the anonymity provided by the VPN tunnel.

**ProtonVPN Client in Disconnected State**



This screenshot shows the ProtonVPN client interface when disconnected from the VPN server. The application displays "Unprotected" status with a red indicator, and shows the original IP address (49.37.132.94) from India with Jio as the provider. The interface is ready to connect with the "Connect" button visible, and the "Fastest free server" option is selected with auto-selection from available countries. This state represents the unprotected browsing condition without VPN encryption.

**IP Address Verification After VPN Disconnection**

****

This final screenshot confirms the return to the original IP address and location after disconnecting from the VPN. The IP address has reverted to 49.37.132.94, with the ISP shown as Reliance Jio Infocomm Limited and location back to Nanakramguda, Telangana, India. The website no longer detects VPN usage, showing the warning "Your location may be exposed!" This demonstrates that the VPN connection can be reliably established and terminated, with the system returning to its original network configuration.

**7. What are some VPN limitations?**

* **Speed reduction is inevitable** - Since your internet traffic has to travel through an extra server and get encrypted/decrypted, you'll always experience some slowdown. Free VPNs like ProtonVPN typically have more speed limitations compared to paid services.
* **Not all websites play nice with VPNs** - Some streaming services (like Netflix), banking websites, and online stores actively block VPN traffic. You might find yourself unable to access certain content or having to constantly prove you're not a robot through captcha tests.
* **Free services come with strings attached** - Most free VPNs have data limits, fewer server locations, and slower speeds. Some questionable free VPN providers might even log your activity or show you ads, defeating the purpose of using a VPN for privacy.
* **It's not a magic invisibility cloak** - While VPNs hide your IP address, they don't make you completely anonymous online. Websites can still track you through cookies, browser fingerprinting, and your login accounts. A VPN is just one piece of the privacy puzzle.

**8. How does a VPN affect network speed?**

* **The encryption overhead** - Your internet traffic needs to be encrypted before leaving your device and decrypted when it reaches the VPN server. This extra processing takes time and computational power, naturally slowing things down. It's like having to translate every conversation through a secure code.
* **The extra distance your data travels** - Instead of your data going directly from your device to a website, it now has to make a detour through the VPN server first. If you're connecting to a server in another country (like I did with the Netherlands server), your data is literally traveling thousands of extra miles.
* **Server congestion matters** - Popular free VPN servers can get crowded, just like a highway during rush hour. When I was connected to the Netherlands server, it was running at 79% capacity, which means other users were sharing the same server resources, potentially affecting my speed.
* **The good news** - For regular browsing, emailing, and social media, the speed difference is usually manageable. You'll mainly notice it when downloading large files, streaming high-quality videos, or gaming online. Most people find the privacy benefits worth the minor speed trade-off for everyday internet use.