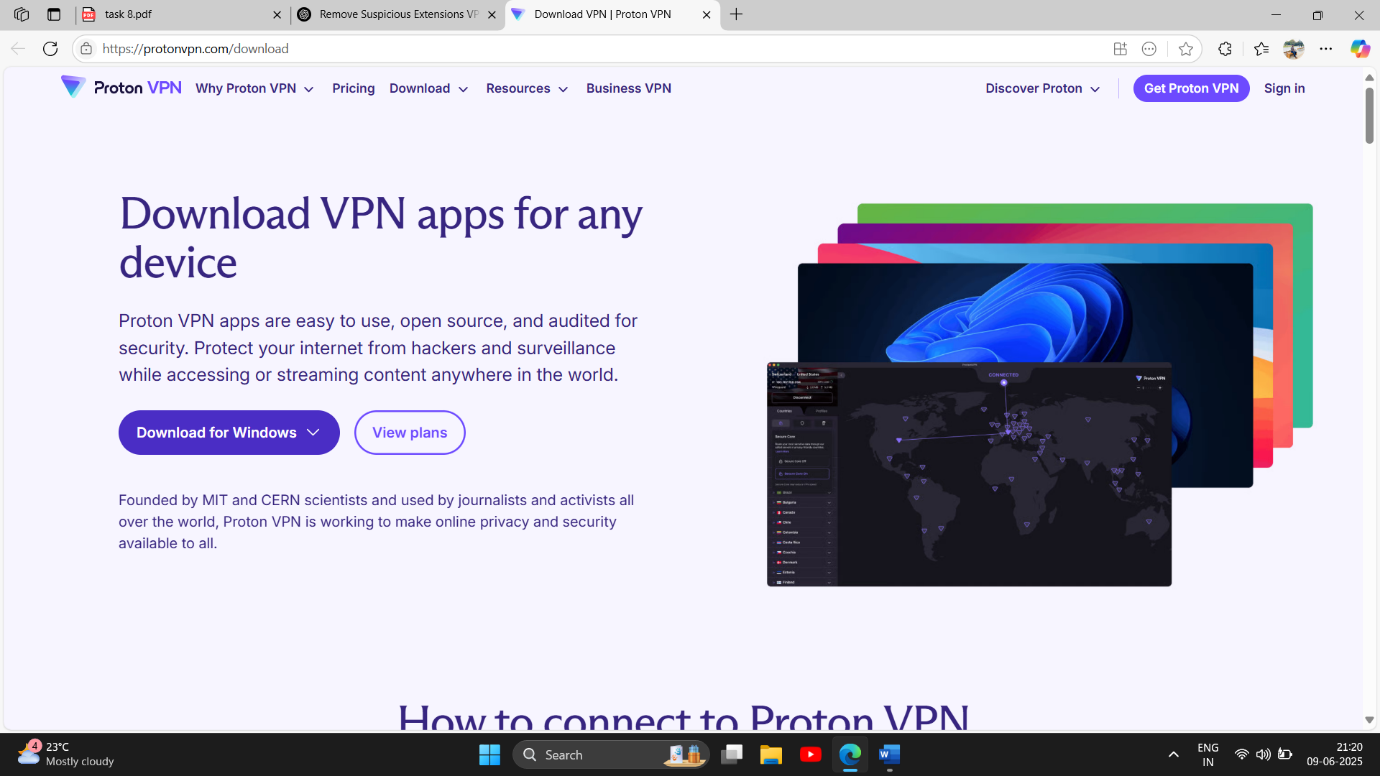
**VPN Privacy and Secure Communication Report**

Objective:

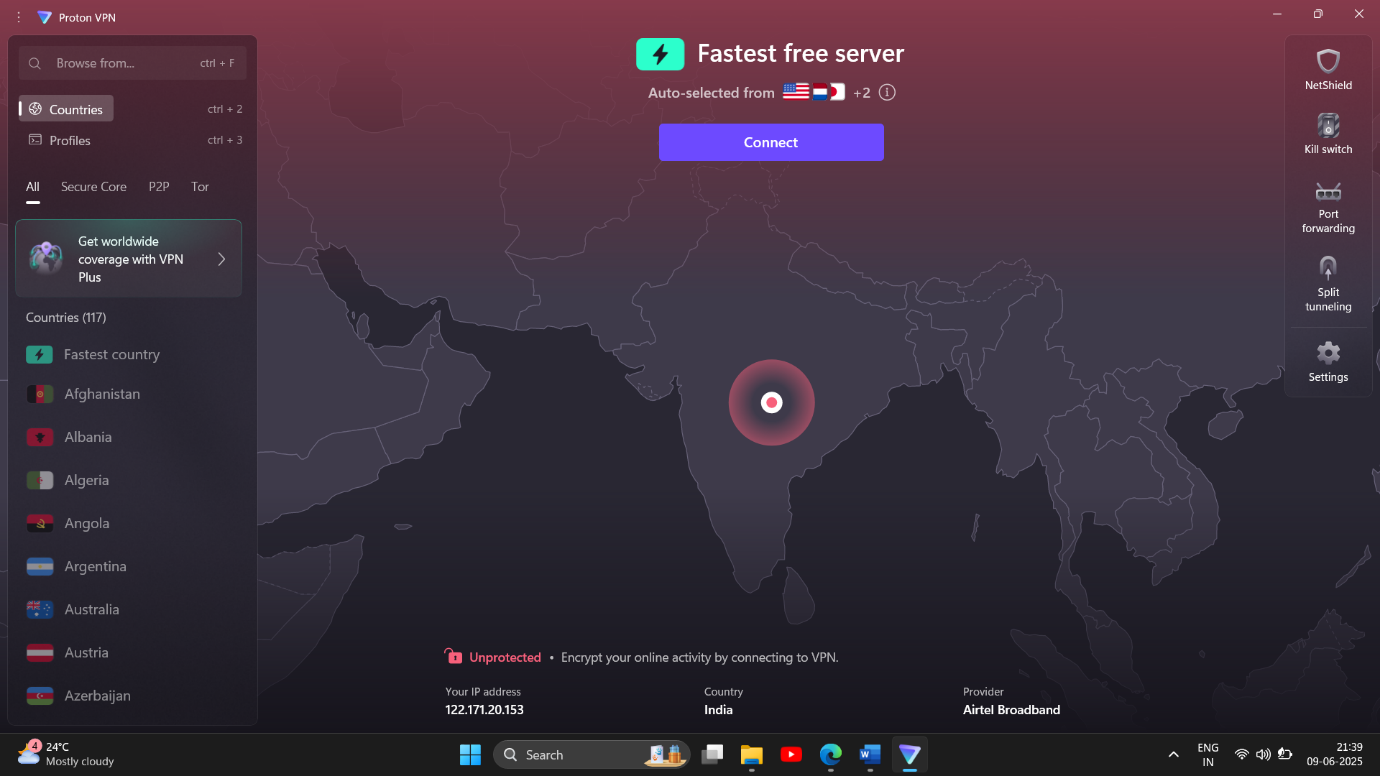
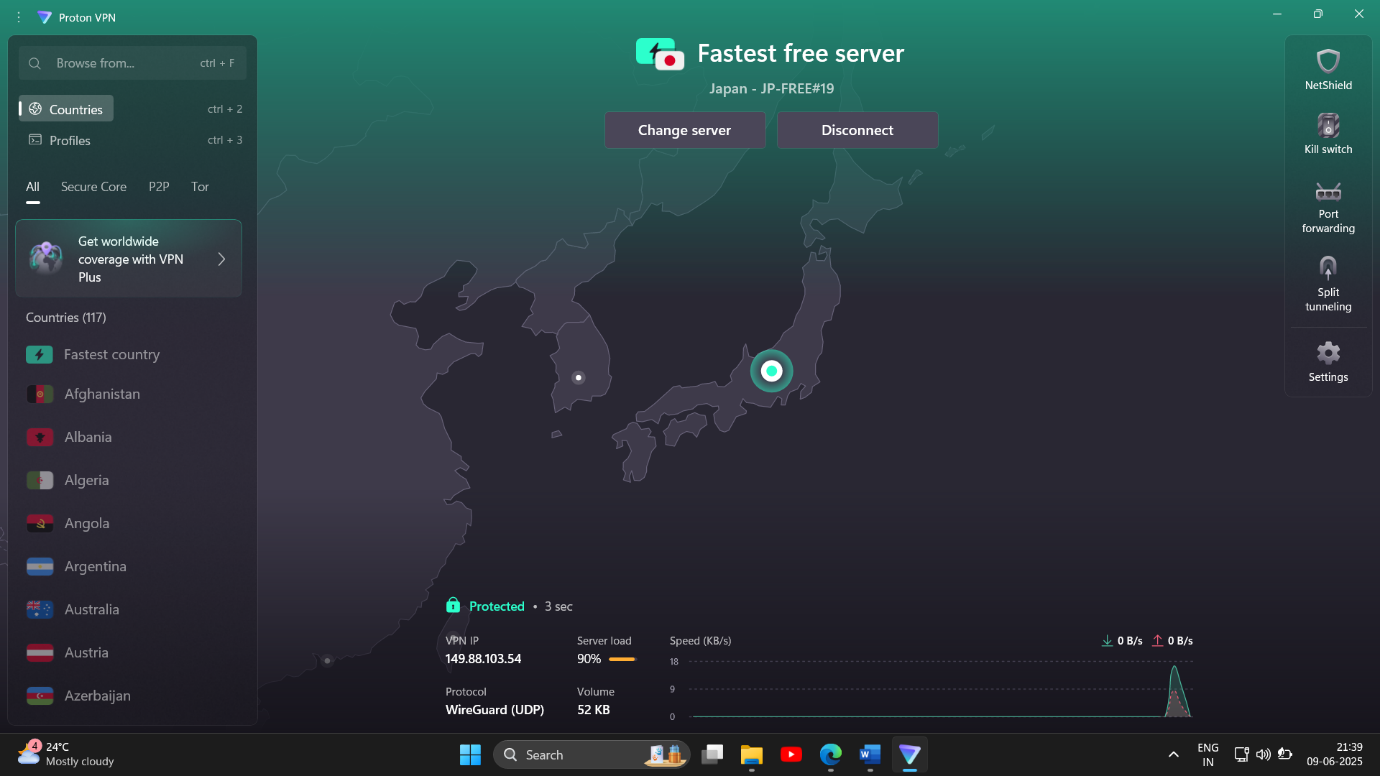
Understand how VPNs protect online privacy and enable secure communication by setting up and testing a free VPN service.

Chosen VPN: ProtonVPN

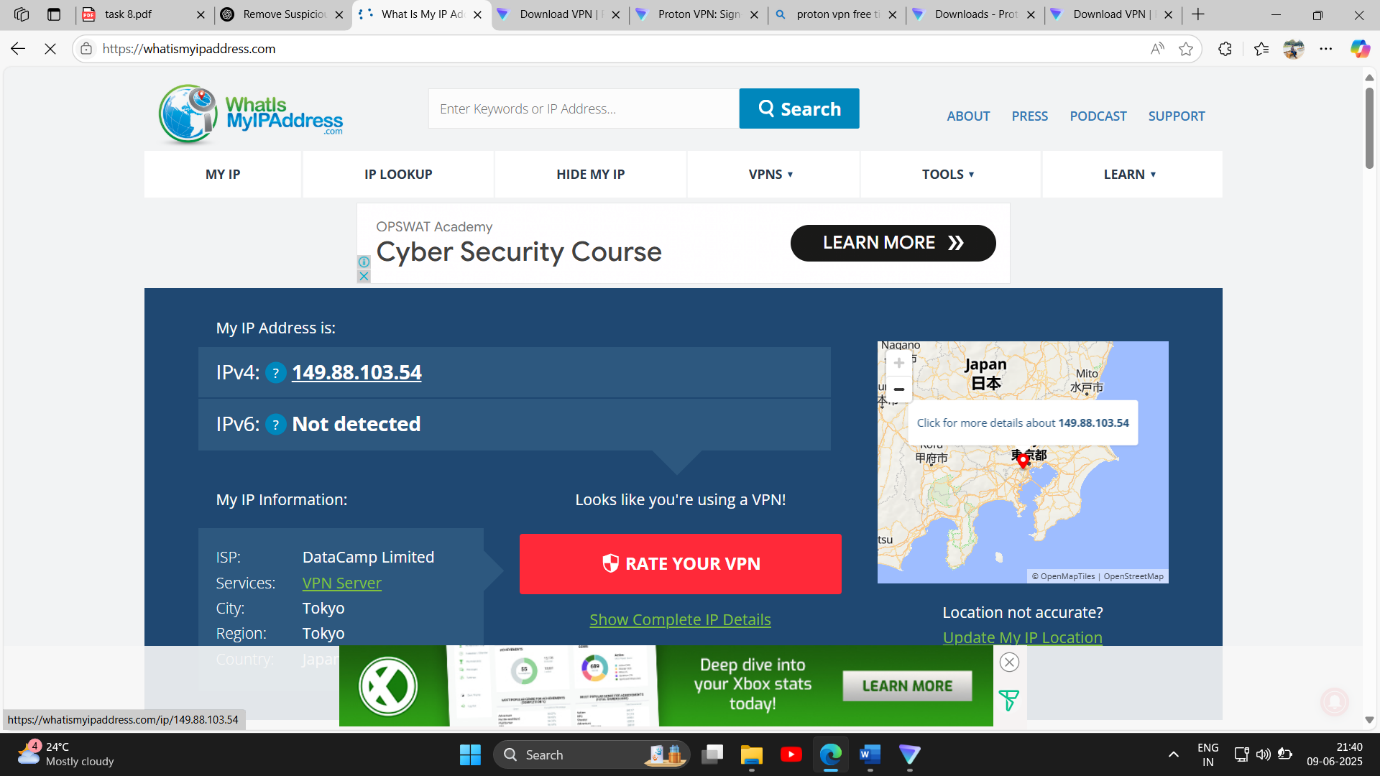
1. Download and Install the VPN Client

* Platform: Windows
* Downloaded from: https://protonvpn.com/download
* Successfully installed ProtonVPN app.
* 

2. Connect to a VPN Server

* Logged into ProtonVPN using registered free account.
* Connected to the Netherlands server (one of the free options).
* Connection status: ✅ Connected
* 
* 

3. Verify IP Address Has Changed

* Visited <https://whatismyipaddress.com>
* New IP was visible, different from my actual ISP-provided IP.
* Location shown as Netherlands confirming the VPN routing.
* 

4. Confirm Encrypted Traffic

* Browsed multiple websites including Google, YouTube, and ProtonMail.
* All traffic remained encrypted and accessible.
* No DNS leaks or disruptions noticed.

5. Research VPN Encryption & Privacy Features

* Encryption Standard: AES-256-bit encryption
* Protocols Used: OpenVPN, WireGuard (on select platforms)
* No-Logs Policy: ProtonVPN does not log user activity.
* DNS Leak Protection: Enabled by default
* Kill Switch: Available in settings (disables internet when VPN disconnects unexpectedly)

VPN Benefits

* Encrypts all traffic, protecting data on public networks.
* Masks IP address to prevent tracking and profiling.
* Enables secure remote access to sensitive systems.
* Bypasses geo-restrictions and censorship.
* Protects against man-in-the-middle (MITM) attacks.

VPN Limitations

* Free versions may offer limited servers and speed.
* Slightly slower browsing/download speeds due to encryption overhead.
* Does not protect against malware/phishing if users visit harmful sites.
* Can be blocked by some websites or streaming services.