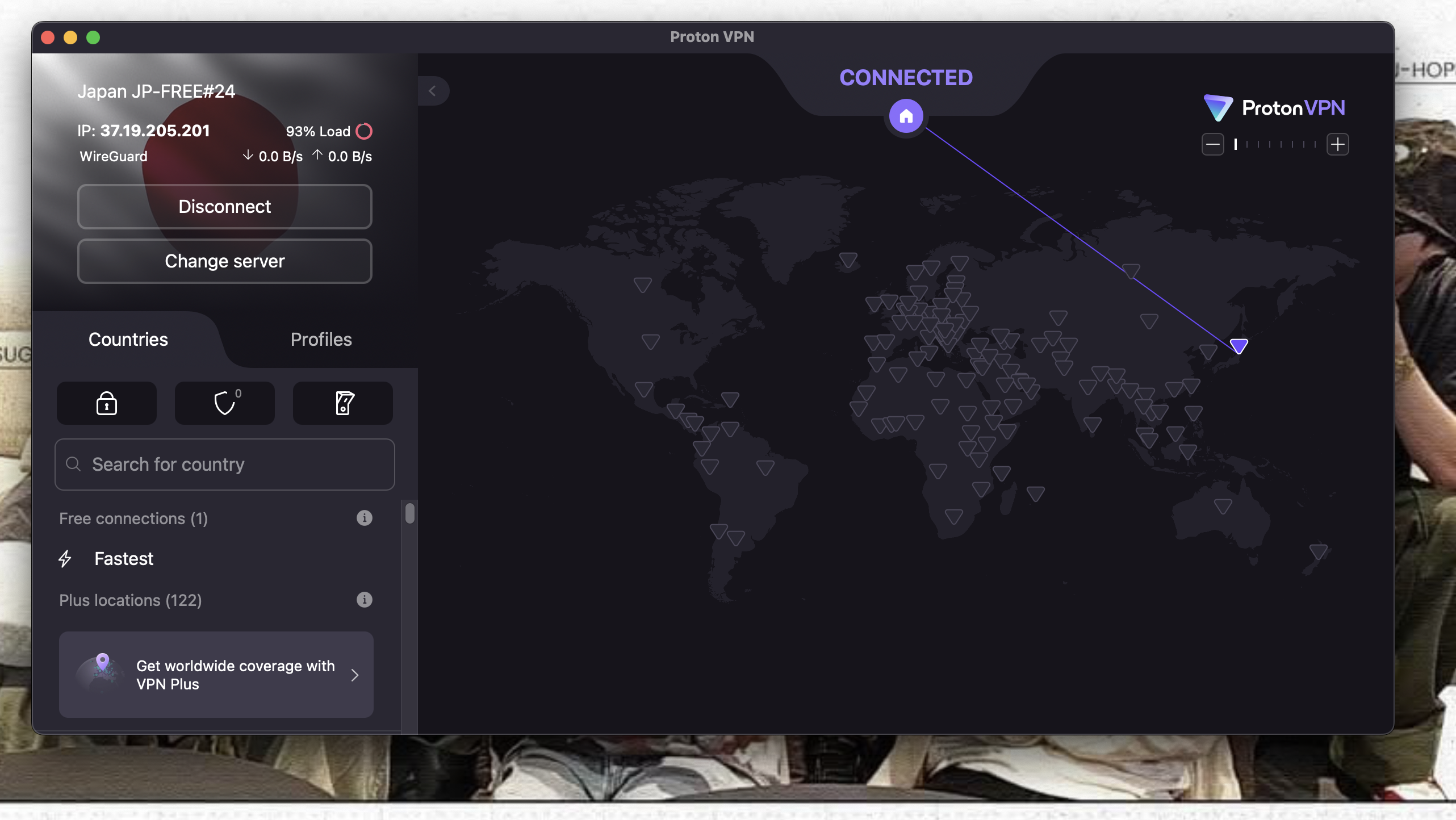
Task 8: Working with VPNs

* Selected ProtonVPN free tier for this task due to its reputation and no data limits.
* Downloaded the ProtonVPN application from the official website.
* Installed the client on the device following the installation prompts.
* Opened the ProtonVPN client.
* Logged in using the ProtonVPN account.
* Connected to a free VPN server located in Japan (Server: Japan JP-FREE#24).
* Screenshot taken showing "Connected" status with server IP: 37.19.205.201 using the WireGuard protocol.
* 
* Visited [whatismyipaddress.com](https://whatismyipaddress.com/) or similar IP checker.
* Confirmed the IP address changed from the original to the VPN-assigned IP address (37.19.205.2
* Browsed the non-HTTPS website <http://httpforever.com/>.
* Noted the browser showed “Not Secure,” indicating HTTP without encryption at the website.
* Despite this, with VPN connected, traffic is encrypted between the device and VPN server (not visible to local network).
* Disconnected ProtonVPN.
* Confirmed real IP address was visible again .
* Compared browsing speed between connected and disconnected states (observed normally faster speed when disconnected, due to no VPN overhead).

## VPN Encryption and Privacy Features

* VPN uses WireGuard protocol providing secure, fast, and encrypted tunneling.
* VPN traffic is encrypted on the user-to-server path, protecting against eavesdropping on unsecured networks.
* VPN masks the user’s IP address and location.
* Limitations include potential speed decrease and no full anonymity since traffic leaves VPN server unencrypted on non-HTTPS sites.

## VPN Benefits:

* Privacy Protection: Masks your real IP address, helping to keep your identity and location private online.
* Data Encryption: Encrypts your internet traffic, securing communications from eavesdroppers, hackers, and ISPs—especially on unsecured networks (like public Wi-Fi).
* Bypass Geo-Restrictions: Allows you to access content, websites, and online services restricted by your geographical location.
* Prevents ISP Tracking: Stops your internet service provider from seeing your browsing activity and history.
* Secures Public Networks: Protects you when using public Wi-Fi at cafes, airports, hotels, etc.
* Remote Access: Enables safe access to private networks (e.g., company intranet) from outside locations.

## VPN Limitations

* Not Absolute Anonymity: The VPN provider itself can see your real IP and potentially log your activity; full anonymity is not guaranteed.
* Speed Reductions: VPNs may reduce download/upload speeds due to encryption and routing overhead, especially on free or overloaded servers.
* No Protection Beyond VPN Server: For non-HTTPS sites, traffic between the VPN server and the destination website remains unencrypted and exposed.
* Potential Trust Issues: Users must trust the VPN provider with their data and privacy.
* Blocked by Some Services: Some websites or streaming platforms block traffic from known VPNs.
* Limited Device Support: Not all devices or network setups support VPNs easily.
* VPN Legality: Usage may be restricted or illegal in certain countries.