# Task 8: Working and understanding VPN

## Download and install VPN service

For this task we will download Proton VPN from <https://protonvpn.com/download>. First, signup on proton VPN website.

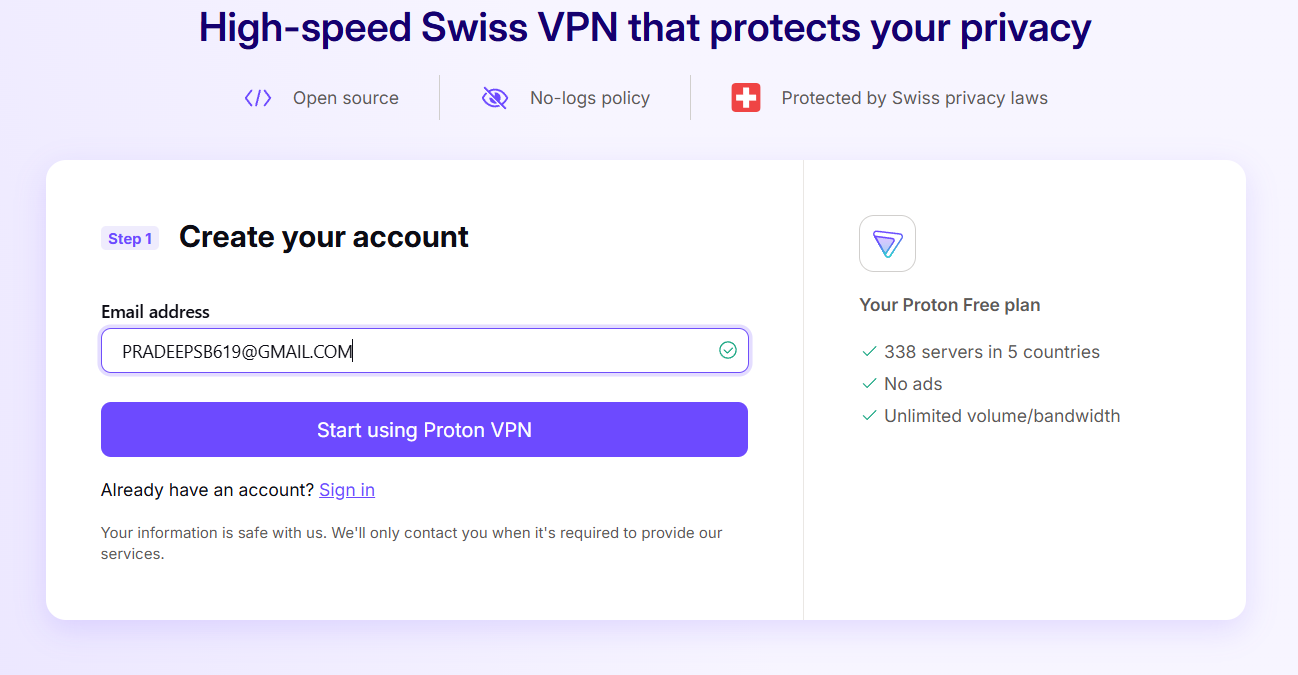


Figure - Signing up for Proton VPN access

A screenshot of a computer

AI-generated content may be incorrect.

Figure - Email verification for Proton VPN access

Then download the VPN app for windows.

A screenshot of a computer

AI-generated content may be incorrect.

Figure - Download VPN for windows from the website



Figure - Welcome page of Proton VPN app on windows

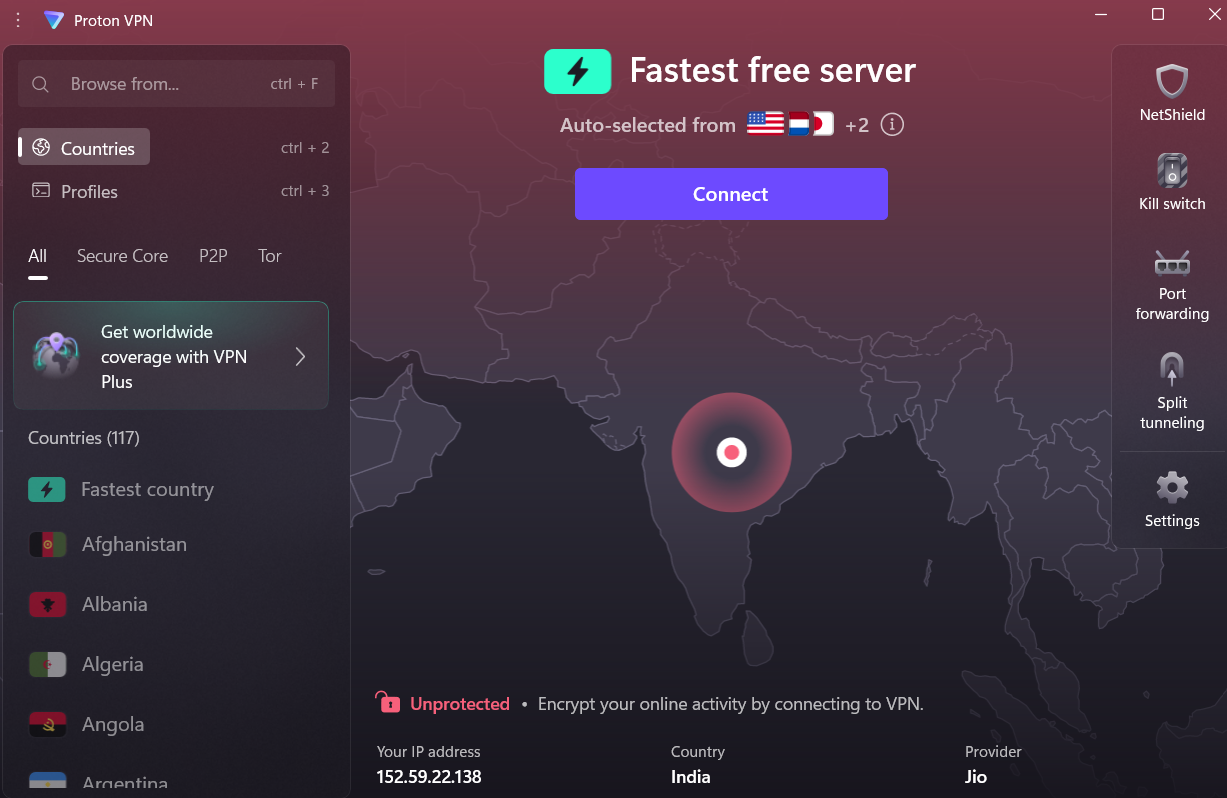


Figure - Proton VPN after installation on windows

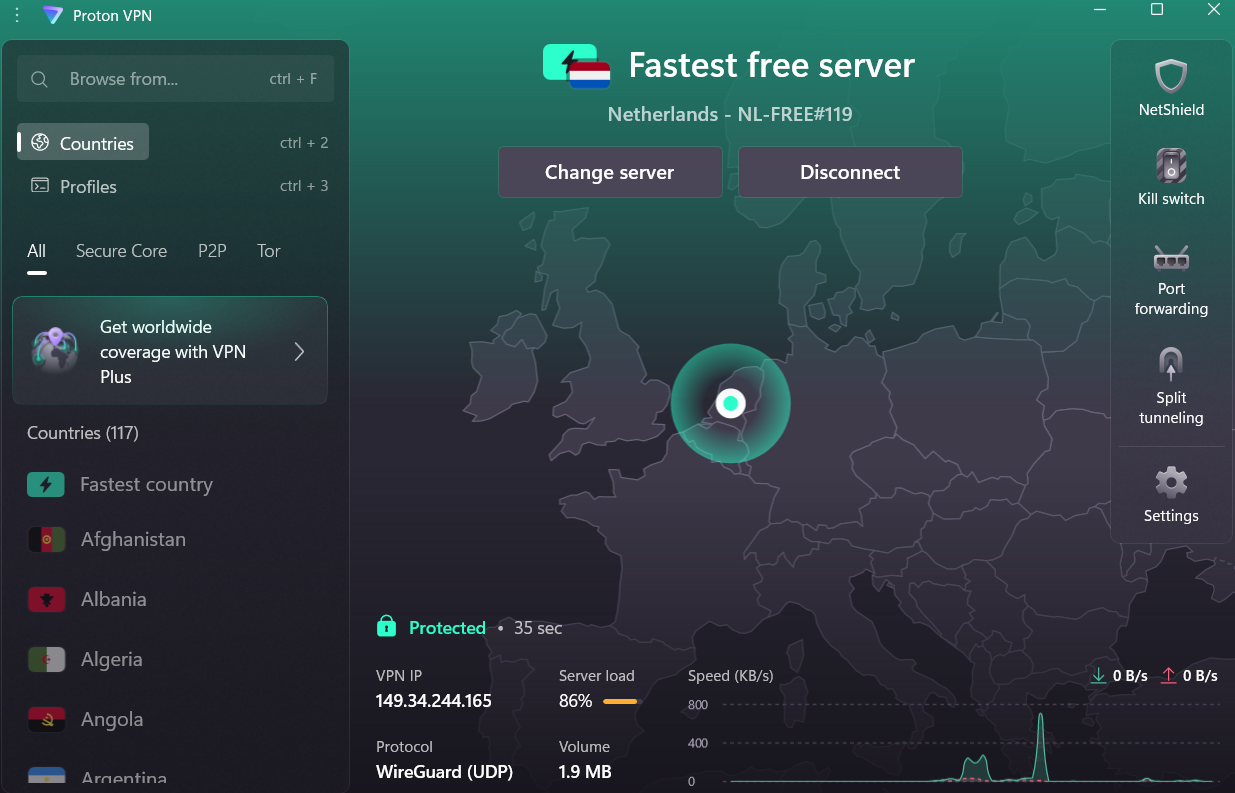


Figure - Active VPN from Netherlands server

## Verify Change of IP address by using the VPN



Figure - IP address of the device before Proton VPN

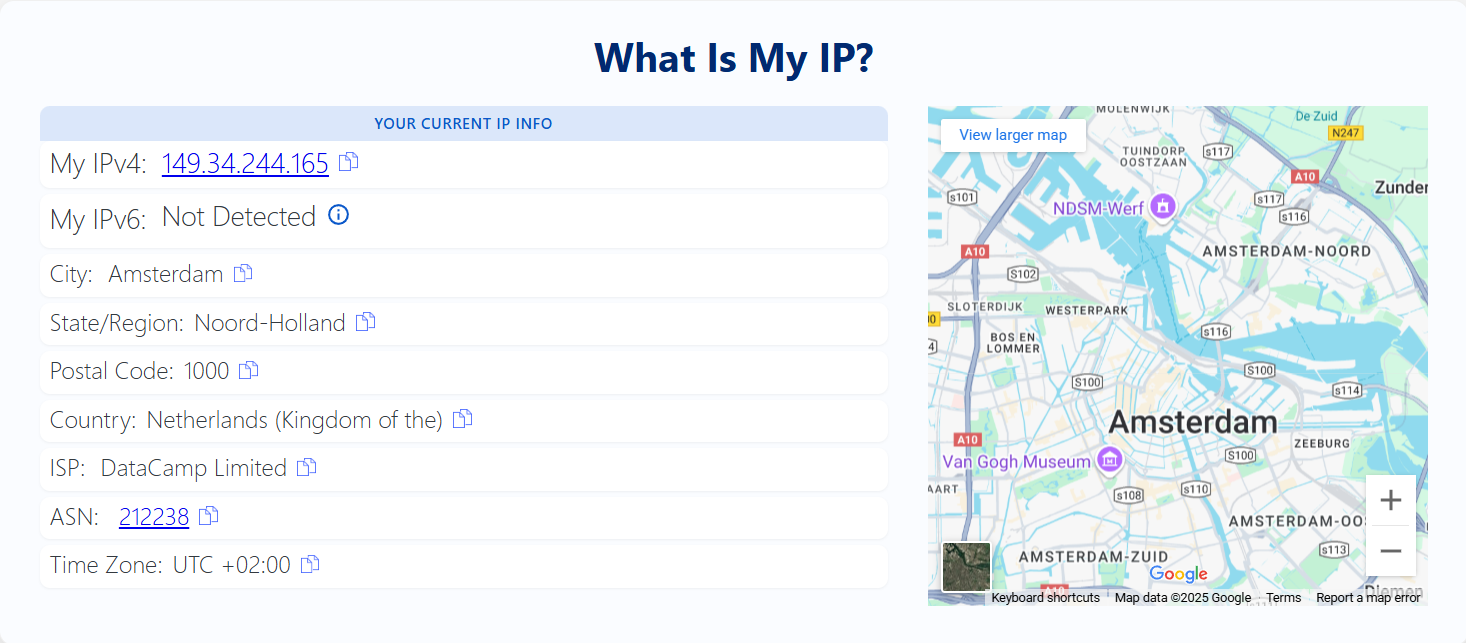


Figure - IP address of device after Proton VPN use

## Confirm encrypted traffic from the VPN

In the URL, HTTPS indicates that the traffic is encrypted.

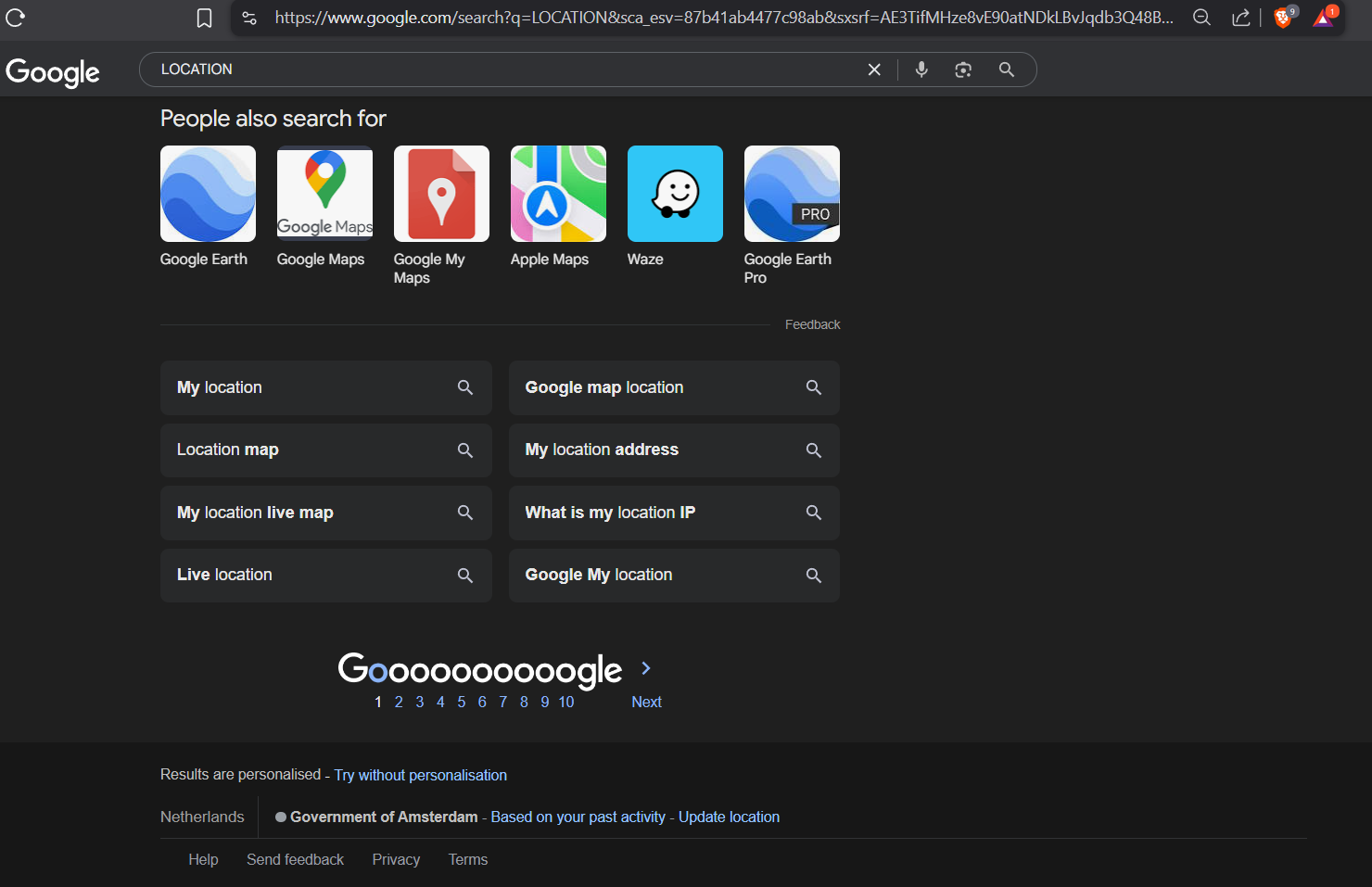


Figure - Confirmation of encrypted traffic from surfing

## Compare browsing speed

Internet speed test from <https://www.speedtest.net/>

### Before Proton VPN

A screenshot of a computer

AI-generated content may be incorrect.

Figure - Speed test result **before** the VPN access

### After Proton VPN

Screens screenshot of a computer

AI-generated content may be incorrect.

Figure - Speed test **while using Proton** VPN

As you can see from figure 10 and 11 internet speed reduced after use of VPN.

## Encryption and Security Features for Proton VPN

### 1. Encryption Standards

* **AES-256**: Industry-standard symmetric encryption considered unbreakable by brute force with current technology.
* **RSA-4096**: Used for key exchange, providing strong asymmetric encryption.
* **HMAC with SHA-512**: Ensures data integrity and authentication.

### 2. VPN Protocols Supported

* **OpenVPN (UDP/TCP)**: Highly secure and widely audited.
* **IKEv2/IPSec**: Fast and reliable, especially on mobile networks.
* **WireGuard**: Offers high speed with strong encryption, used under Proton VPN’s **Stealth** protocol.
* **Stealth Protocol** (Proton’s proprietary): Helps bypass censorship and VPN blocks by disguising VPN traffic as HTTPS.

## Privacy Features

### 1. No-Logs Policy

* Proton VPN maintains a **strict no-logs policy**.
* No user activity, connection logs, or IP addresses are stored.
* Independent security audits confirm this policy.

### 2. Secure Core

* Routes traffic through **multiple servers** (usually in privacy-friendly countries like Switzerland, Iceland, or Sweden) before reaching the internet.
* This provides protection against **network-level surveillance** and **correlation attacks**, especially if the exit server is compromised.

### 3. Perfect Forward Secrecy

* Ensures session keys are **temporary**. Even if one session key is compromised, previous sessions remain secure.

### 4. Kill Switch + Always-on VPN

* Prevents data leaks if the VPN connection drops.
* Ensures your device is **never exposed** to the internet without protection.

### 5. DNS Leak Protection

* Proton VPN routes all DNS queries through its **encrypted VPN tunnel**, ensuring **no DNS requests** are leaked to your ISP.

### 6. Tor Over VPN

* Direct access to the **Tor network** through Proton VPN.
* Helps maintain anonymity by adding another layer of obfuscation.

### Independent Audits and Open Source

* Proton VPN apps are **fully open-source**, allowing the public to verify their security.
* Underwent **independent security audits** (e.g., by SEC Consult).
* Complies with GDPR and is part of the **EU Data Protection Framework**.

## Benefits of a VPN

### 1. Online Privacy

* Hides your **IP address** and location.
* Prevents websites, advertisers, and ISPs from tracking your activity.

### 2. Secure Data Transmission

* Encrypts your internet traffic (e.g., with **AES-256**), protecting sensitive information on **public Wi-Fi** or untrusted networks.

### 3. Bypass Censorship and Geo-Restrictions

* Allows access to websites and services **blocked in your region** (e.g., streaming content, social media).

### 4. Safe Remote Access

* Enables **secure connections** to company networks, useful for remote workers.

### 5. Avoid Bandwidth Throttling

* Prevents ISPs from **slowing down your internet** based on your activity (like streaming or gaming).

### 6. Anonymity with Advanced Features

* Features like **no-logs policies, Tor over VPN**, or **multi-hop routing** increase anonymity.

## Limitations of a VPN

### 1. Not Total Anonymity

* A VPN hides your IP but **doesn't protect you from malware, phishing, or tracking via cookies**.
* Full anonymity requires **Tor, secure browsers, and good privacy practices**.

### 2. Speed Reduction

* Encryption and routing can **slow down internet speed**, especially on long-distance or overloaded servers.

### 3. Trust in VPN Provider

* You must **trust your VPN provider** not to log or misuse your data. A dishonest VPN can become a privacy risk.

### 4. Not a Magic Shield

* VPNs can’t protect against **malware, viruses, or poor security practices**.
* Also, won’t prevent data leaks if you log into accounts tied to your real identity.

### 5. May Be Blocked

* Some services (Netflix, banking apps, governments) may **detect and block VPNs**.

### 6. Legal and Policy Risks

* Using VPNs in **some countries is restricted or illegal**, and misuse (e.g., for criminal activity) has consequences.

## Conclusion

A VPN is a **powerful tool for enhancing online privacy and security**, especially when combined with other measures. However, it is **not a complete solution** for anonymity or protection. Understanding its limitations helps you use it more effectively and safely.