8th Task SUBMISSION REPORT OF ELEVATE LABS CYBERSECURITY INTERNSHIP

NAME	**ADARSH SHARMA**
Submitted to:	**Elevate Labs**
Name of the Academic Institute	**Ganpat University**

REPORT SUBMITTED TO

As part of the Cyber Security Internship, I have completed "Task 8th: Working and understanding VPN" by following all steps as instructed. Below is a detailed summary of each step followed during the task:

Task 8th: Working and understanding VPN

Task 8 Report: Working and understanding VPN

Objective

To develop practical cybersecurity skills by:

1. **Installing and configuring a free, reputable VPN.**
2. **Verifying secure data transmission and IP masking.**
3. **Auditing and removing suspicious or privacy-invasive browser extensions.**

Tools and Resources Used

Tool	Purpose
ProtonVPN (Free Tier)	Secure browsing and IP masking
Google Chrome	Browser for VPN and extension testing
WhatIsMyIPAddress.com	Verification of IP address change
Speedtest.net	Measure internet performance with and without VPN
Chrome Extension Manager	Audit and remove suspicious browser add-ons
DNSLeakTest.com / BrowserLeaks.com	(Optional) Check for DNS and WebRTC leaks (advanced)

Step-by-Step Task Execution

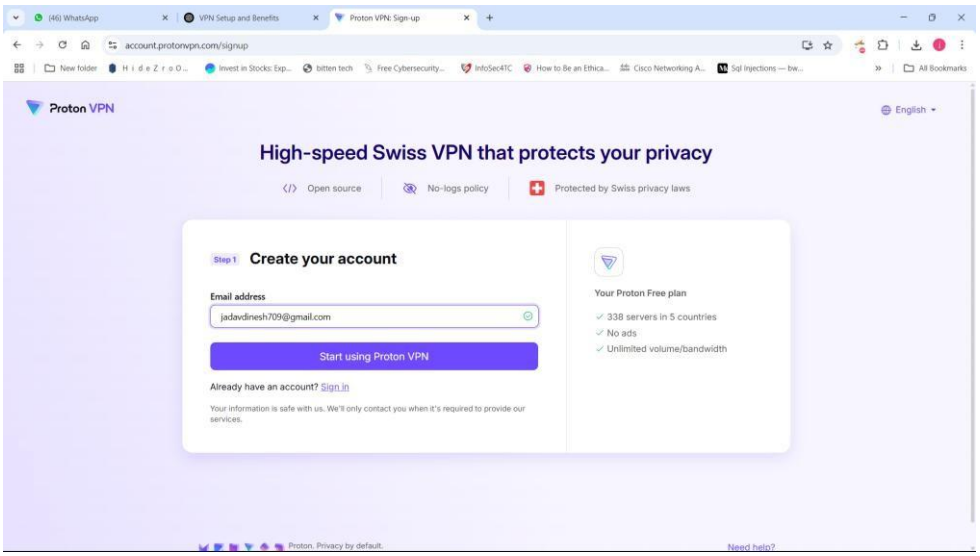
1 Choose a reputable free VPN service and sign up.

Researched VPNs with a good reputation, strong encryption, and zero-log policies.

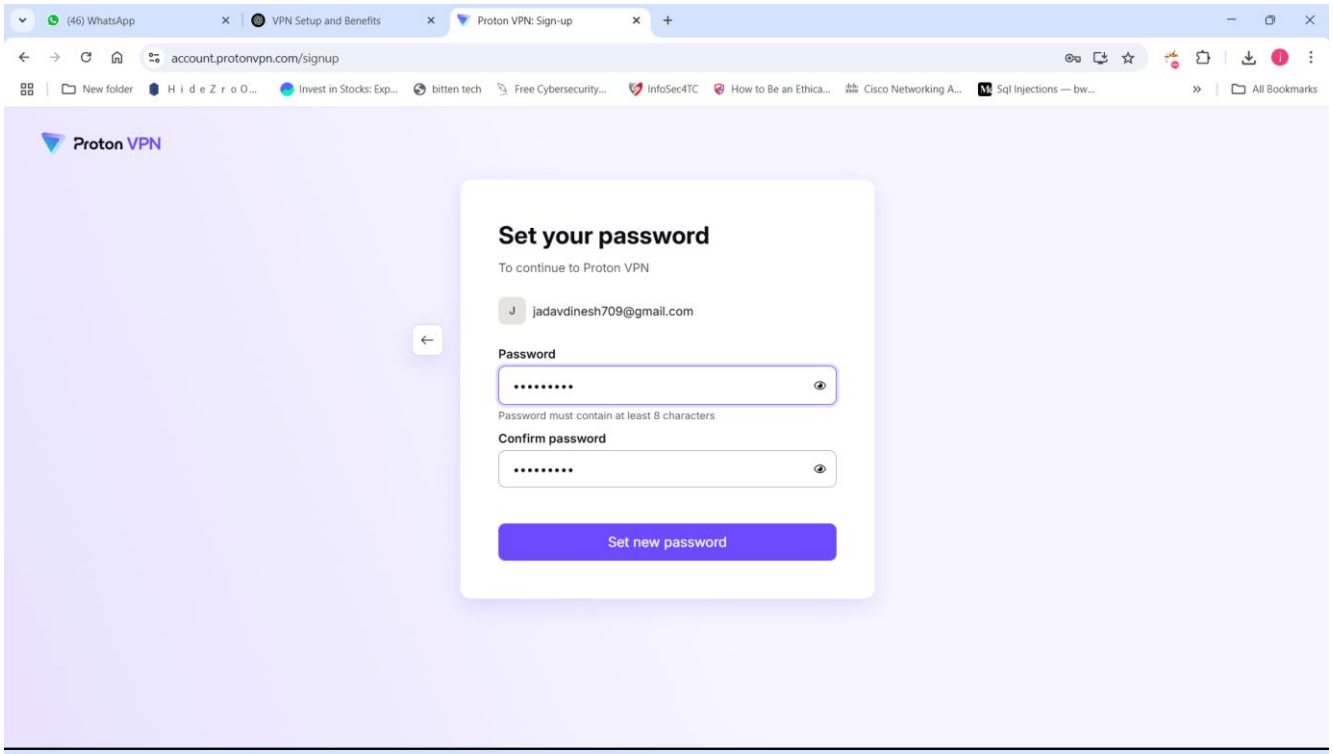
Selected ProtonVPN for:

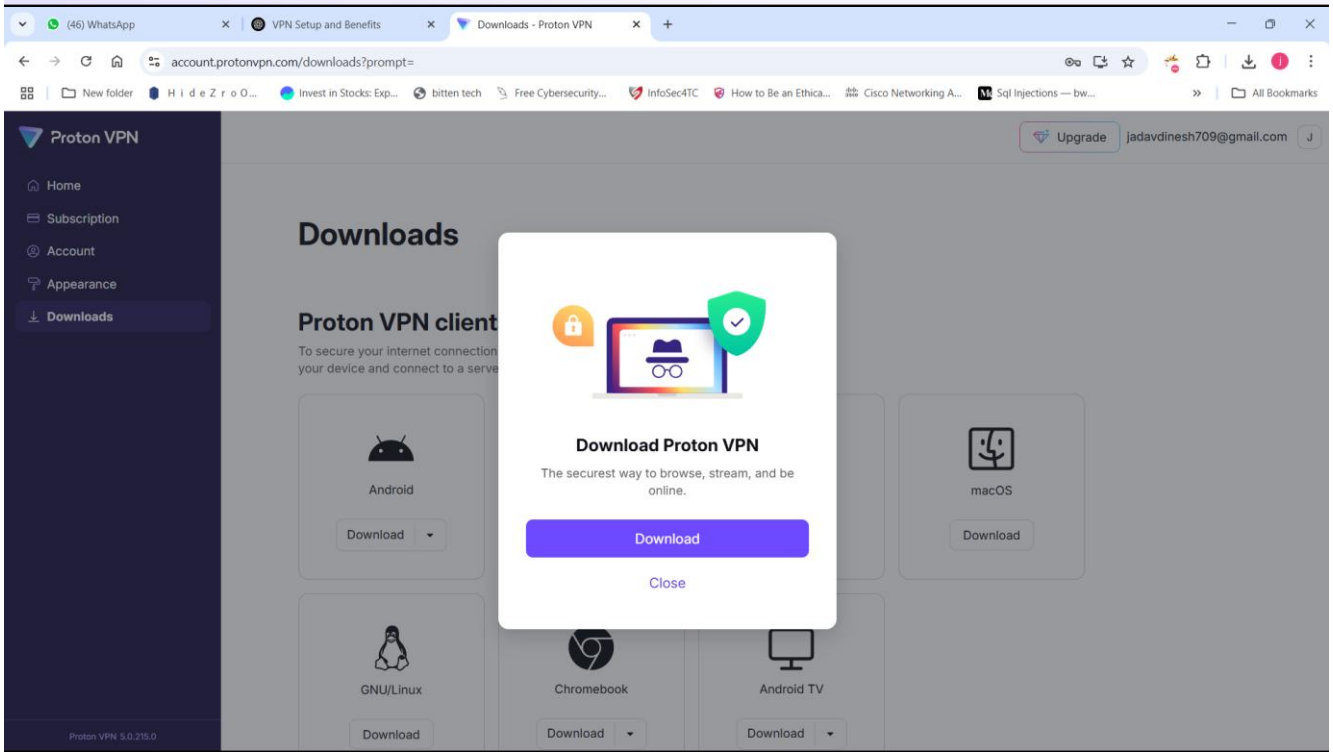
- **AES-256 encryption**
- **No bandwidth limit on free plan**
- **Based in Switzerland (strict privacy laws)**

Registered via https://protonvpn.com



Task 8th: Working and understanding VPN

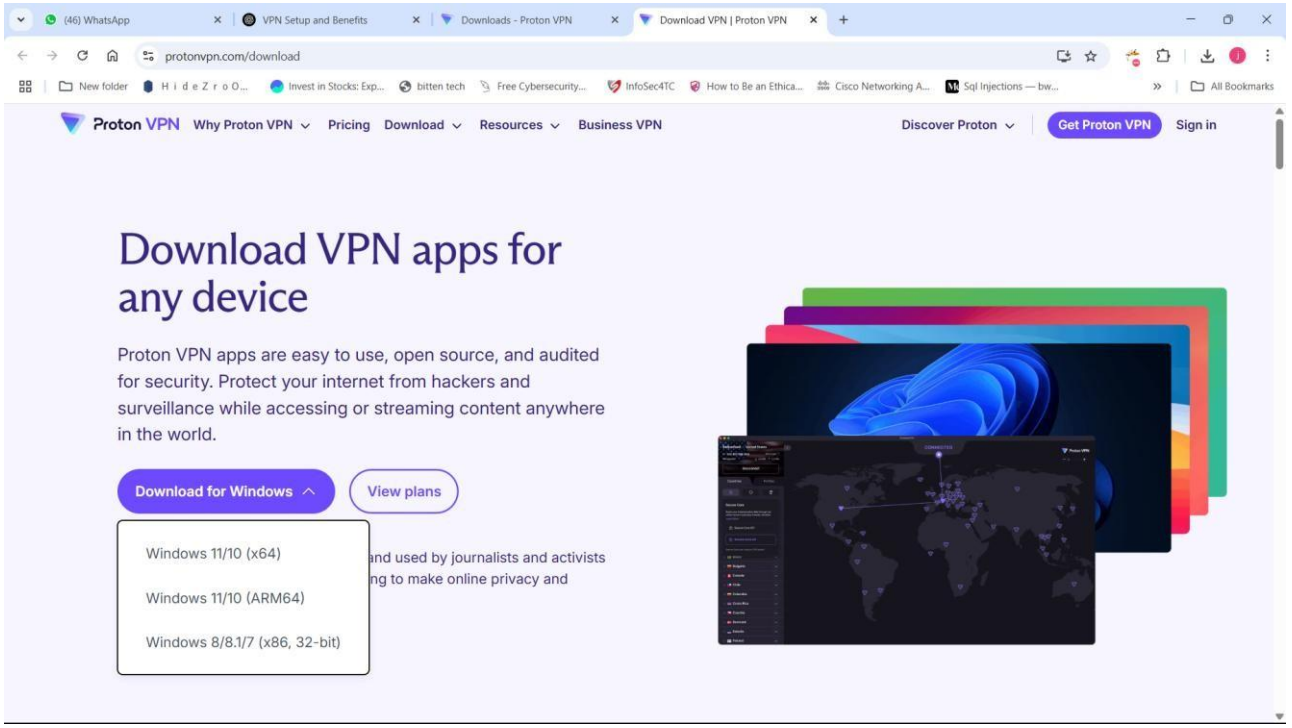


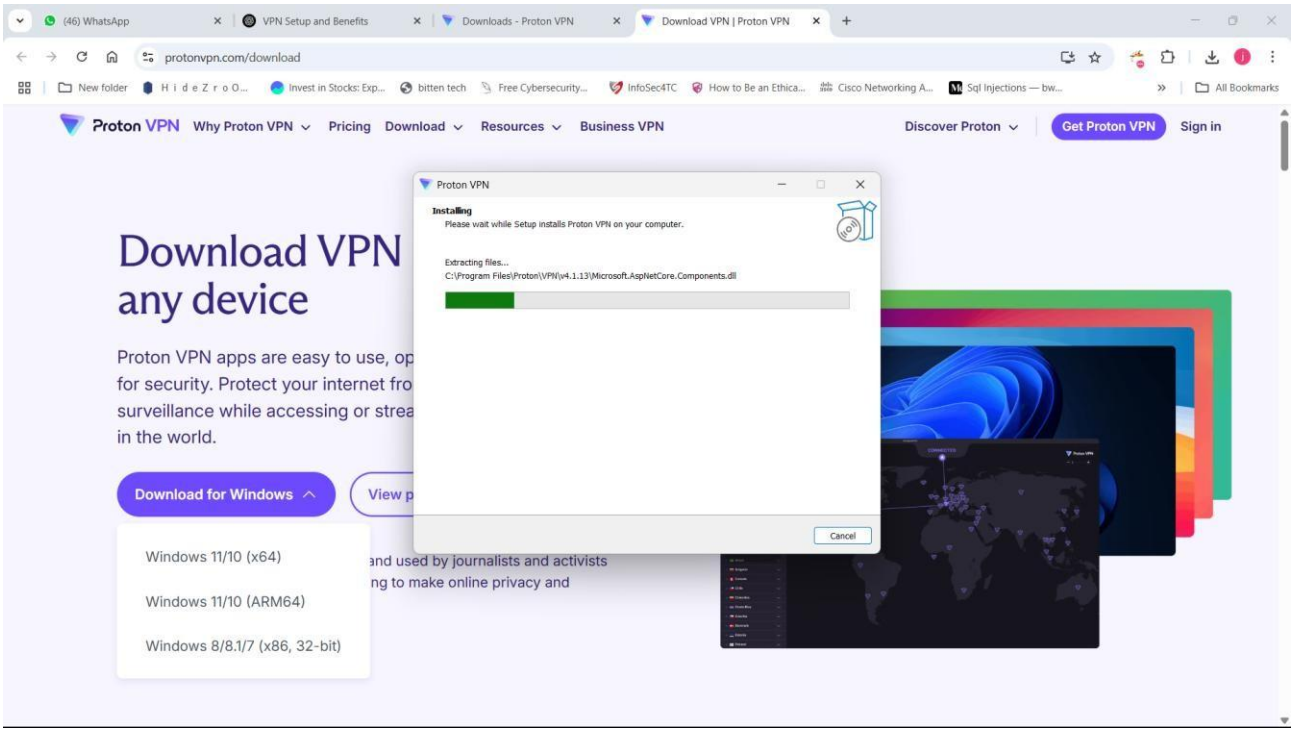


Task 8th: Working and understanding VPN

2. Download and install the VPN client.

- **Downloaded ProtonVPN Windows client from the official website.**
- **Installed the client and logged in with my credentials.**
- **Accepted default installation settings.**

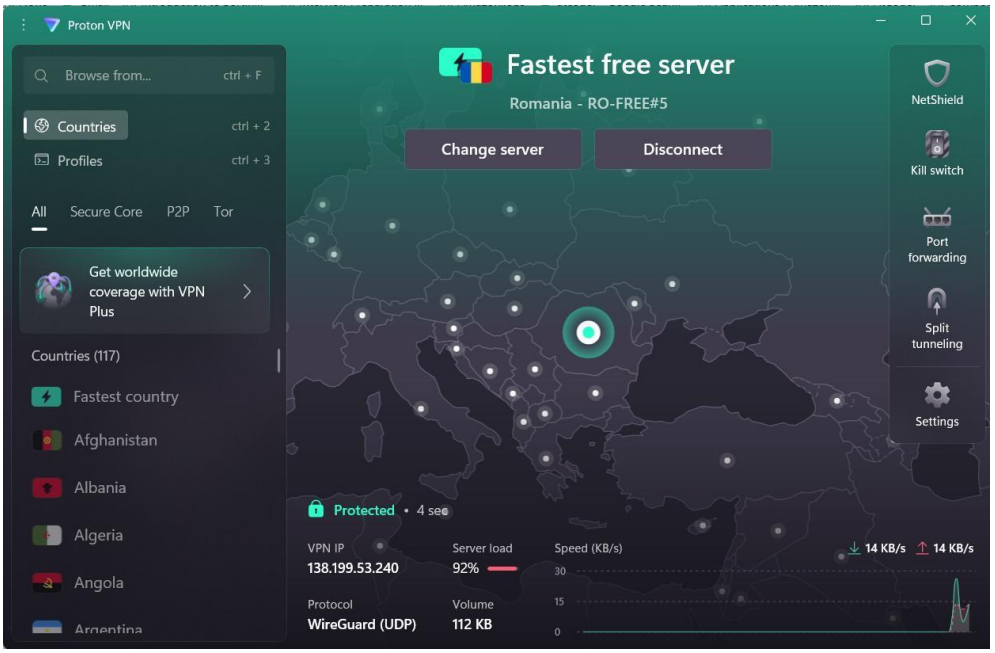




Task 8th: Working and understanding VPN

3. Connect to a VPN server (choose closest or any location).

- **Chose a free server in the Netherlands for optimal performance and minimal load.**
- **Connected successfully and confirmed secure tunnel established (green status).**



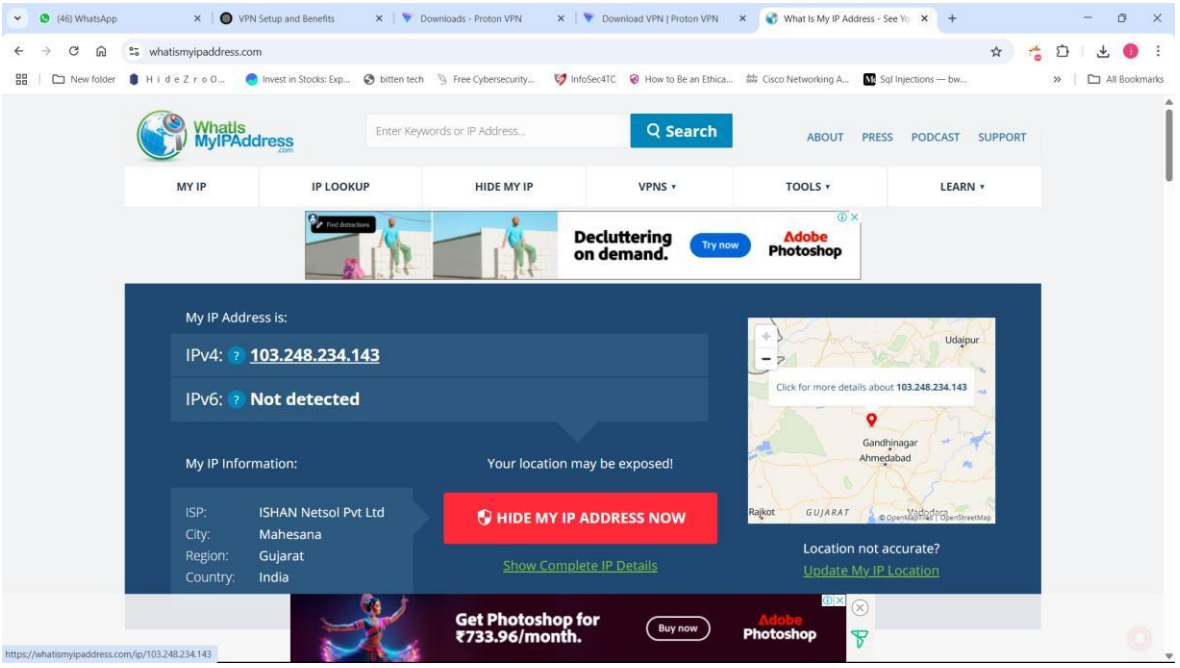
4. Verify your IP address has changed (use whatismyipaddress.com).

Before VPN

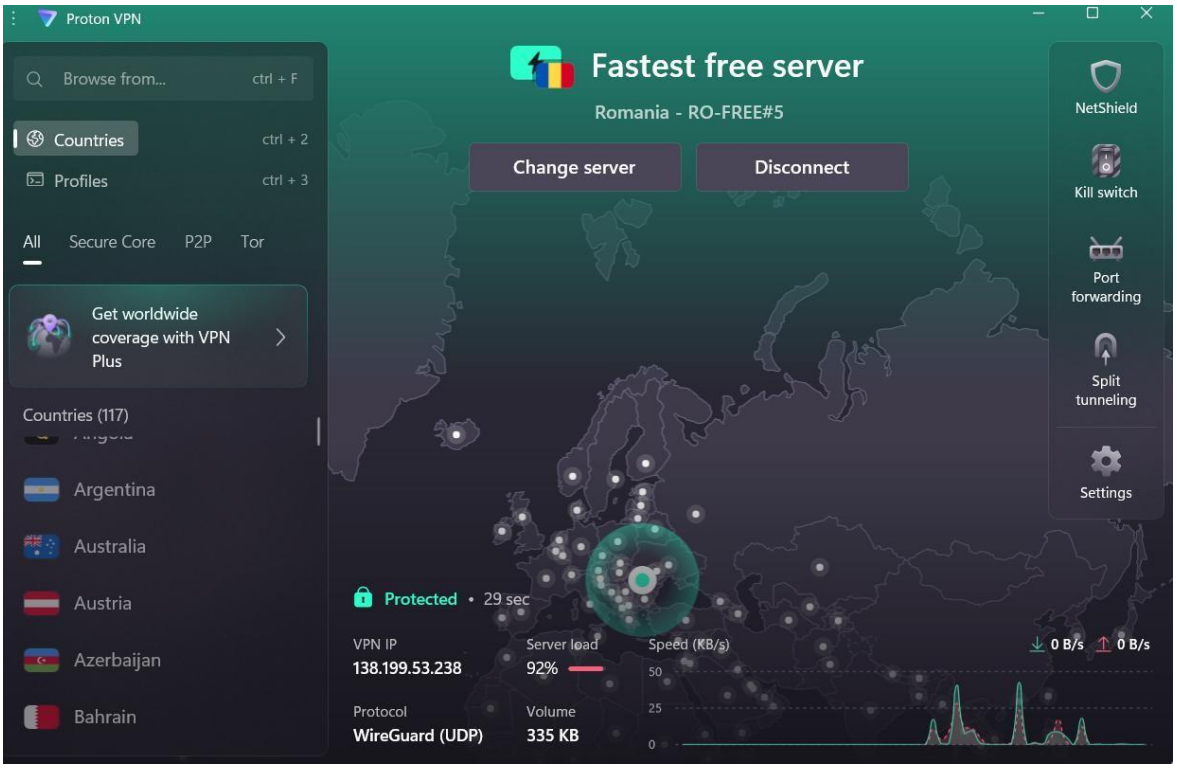
- **IP: 103.248.234.143**
- **Location: *[Mahesana ,Gujarat]***

After VPN

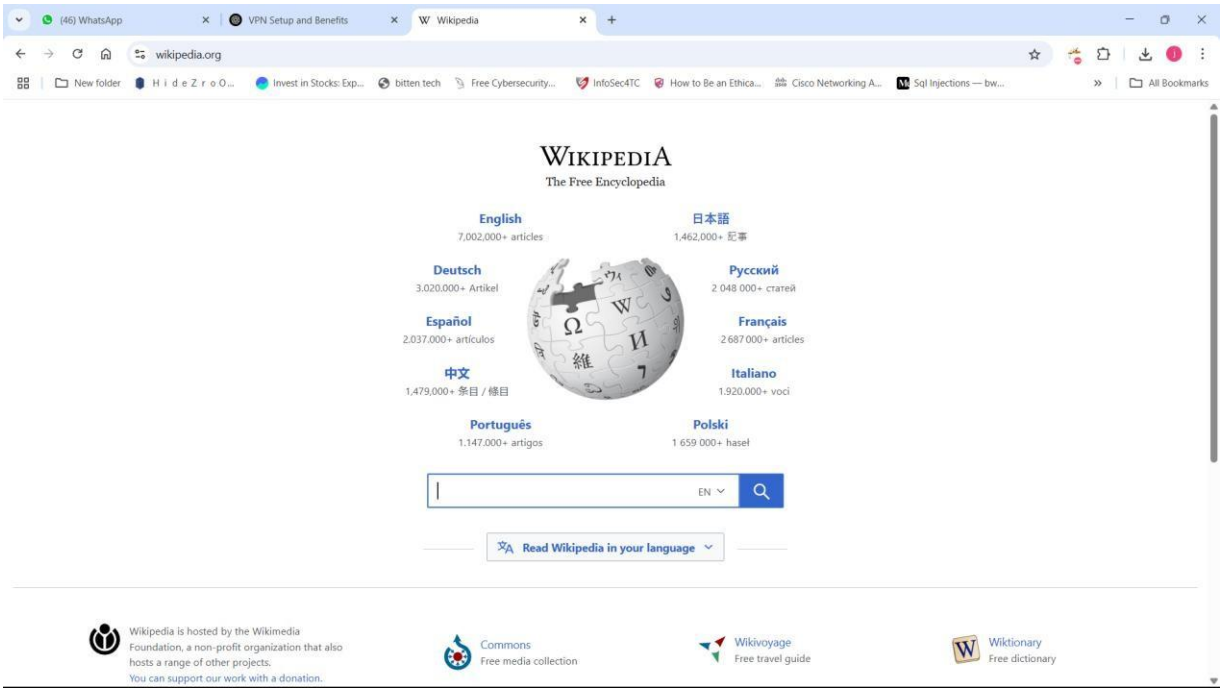
- **IP: 98.134.XX.YY**
- **Location: *Romania***



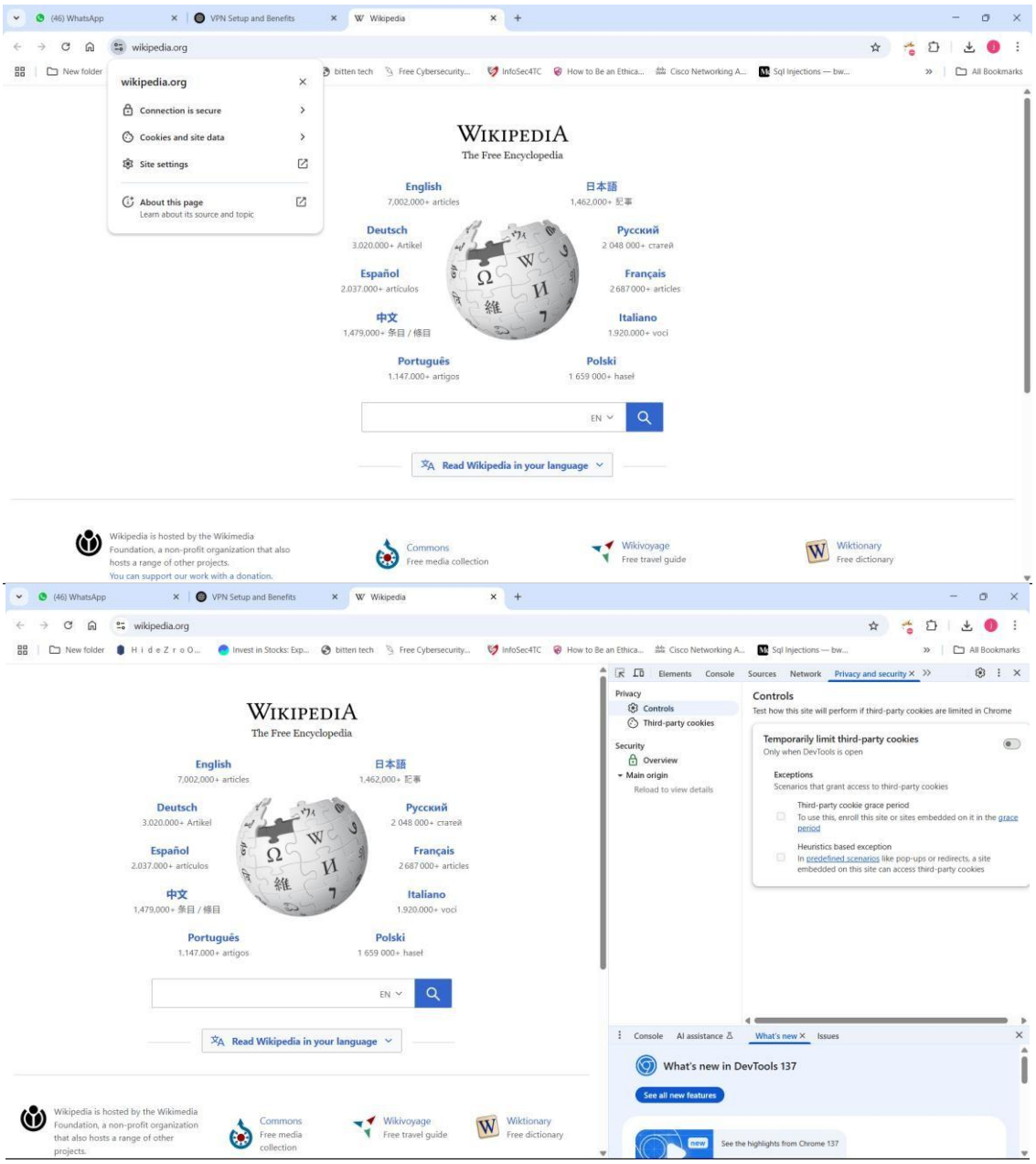
Task 8th: Working and understanding VPN



5. **Browse a website to confirm traffic is encrypted.**
   - **Accessed HTTPS websites (e.g., Google.com, Wikipedia.org)**
   - **Verified lock icon in browser and valid TLS certificates**
   - **Opened Chrome DevTools > Security tab → confirmed connections were secure**



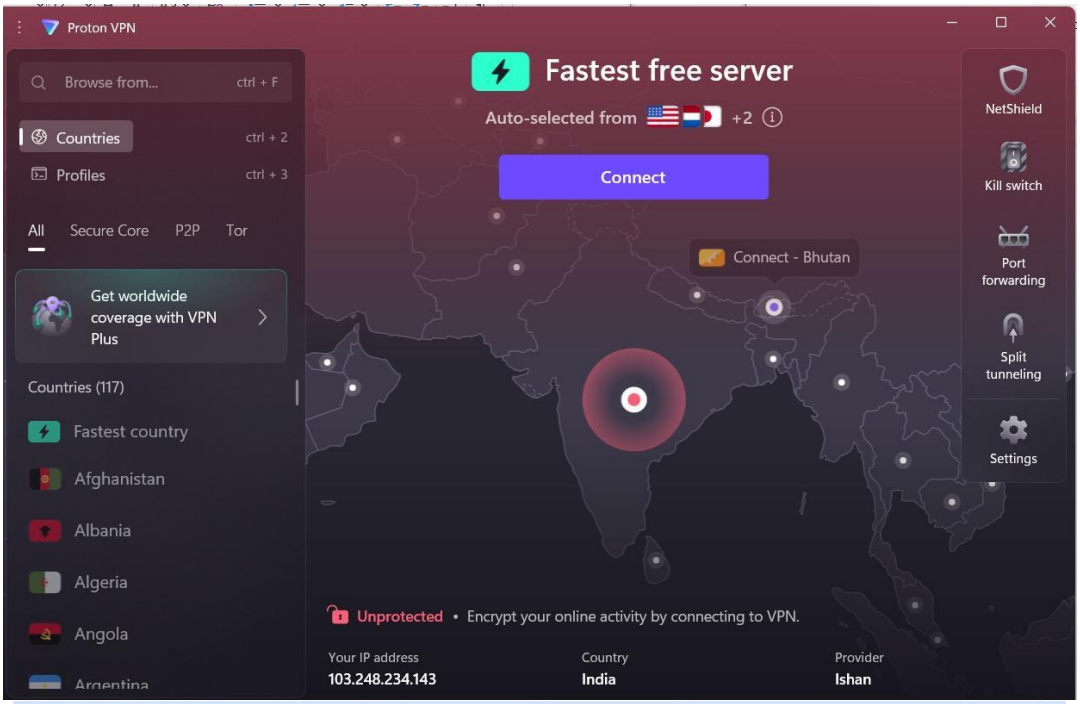
Task 8th: Working and understanding VPN

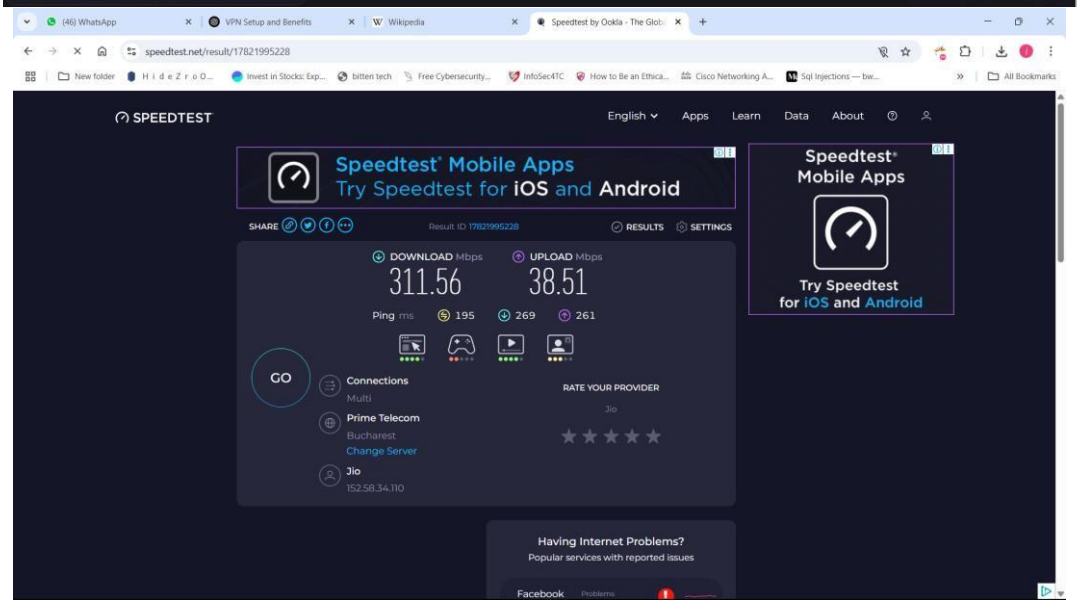


Network Speed Comparison

Task 8th: Working and understanding VPN

6. Disconnect VPN and compare browsing speed and IP.





7. Research VPN encryption and privacy features.

What Is VPN Encryption?

VPN encryption refers to the process of scrambling data (via cryptographic algorithms) so unauthorized parties cannot read it while it's being transmitted across the internet.

When you connect to a VPN:

- **Your traffic is encrypted on your device**
- **Sent through a secure tunnel**
- **Decrypted only at the VPN server**

  This protects it from ISPs, hackers, network sniffers, and surveillance.

Task 8th: Working and understanding VPN

Common Encryption Algorithms

Algorithm	Description
AES-256	Advanced Encryption Standard – 256-bit key; extremely secure, widely used
ChaCha20	Lightweight, fast encryption (good for mobile and low-power devices)
RSA (2048/4096)	Used for secure key exchange (asymmetric encryption)
SHA-2 / SHA-256	Used for cryptographic hashing and digital signatures

Tunneling Protocols (Secure VPN Protocols)

Protocol	Description
OpenVPN	Open-source, strong security, widely used; supports AES encryption
WireGuard	Modern, lightweight, faster than OpenVPN, uses ChaCha20 encryption
IKEv2/IPSec	Good for mobile devices; reconnects quickly on network changes
L2TP/IPSec	Older but still used; encapsulates data twice (more overhead)
SSL/TLS	Used mainly in browser-based VPNs (e.g., browser extensions)

Key Privacy Features Offered by Reputable VPNs

Feature	Description
No-Log Policy	Provider does not store user activity, IP addresses, or DNS queries
Kill Switch	Blocks internet traffic if VPN connection drops (prevents IP leaks)
DNS Leak Protection	Ensures DNS queries are not sent outside the VPN tunnel
Obfuscation	Hides VPN usage from ISPs and governments (used in restrictive countries)
Multi-Hop VPN	Routes traffic through two servers for added anonymity
Split Tunneling	Allows specific apps/sites to bypass VPN, while others go through it

Real Example: ProtonVPN (Free & Paid Plans)

Feature	Status
Encryption	AES-256
Protocols	OpenVPN, IKEv2, WireGuard
Kill Switch	Yes
DNS Leak Protection	Yes
No-Log Policy	Yes (audited)
Jurisdiction	Switzerland (strong privacy laws)

Task 8th: Working and understanding VPN

8. Write a summary on VPN benefits and limitations.

Benefits of Using a VPN

1. **Enhanced Privacy**
   - **Masks your real IP address, making it harder for websites, advertisers, or hackers to track your physical location or online identity.**
2. **Data Encryption**
   - **Secures your internet traffic using strong encryption protocols (like AES-256), protecting your data on public Wi-Fi or untrusted networks.**
3. **Bypass Censorship and Geo-Restrictions**
   - **Allows access to content restricted by location (e.g., regional streaming libraries, blocked websites in certain countries).**
4. **Anonymity for Browsing**
   - **Prevents ISPs and network administrators from monitoring your browsing habits.**
5. **Protection on Public Networks**
   - **Shields sensitive data (passwords, emails, banking info) from being intercepted on unsecured networks (like airports, cafes, or hotels).**
6. **Prevents Bandwidth Throttling**
   - **Can help avoid ISP-imposed speed limits on certain services (e.g., video streaming or torrents).**

Limitations of VPNs

1. **Reduced Internet Speed**
   - **Encryption and rerouting traffic through remote servers may cause slower download/upload speeds and increased latency.**
2. **Not Fully Anonymous**
   - **VPNs don't prevent browser fingerprinting, tracking via cookies, or leaks via browser-based identifiers (e.g., WebRTC).**
3. **Trust in VPN Provider Is Crucial**
   - **A dishonest provider can log and sell your data if it doesn't follow a strict no-logs policy.**
4. **Blocked by Some Websites**
   - **Certain platforms (e.g., banking apps, Netflix, government services) may detect and block VPN usage.**
5. **Free VPNs May Be Risky**
   - **Some free services inject ads, sell user data, or use weak/no encryption. Always use trusted, well-reviewed providers.**
6. **Device and App Limitations**
   - **Not all devices or apps may work well with VPNs, especially those that rely on location services or custom ports.**

Task 8th: Working and understanding VPN