

# ELEVATE LABS

## Cyber Security Internship

INTERN NAME – AMIT MAURYA

### Task 8: VPN Hands-On and Security Understanding

#### Assignment Report

---

#### ❑ Objective

The objective of this task is to gain hands-on experience in setting up and using a VPN to understand how VPNs protect user privacy, secure online communication, and encrypt traffic.

---

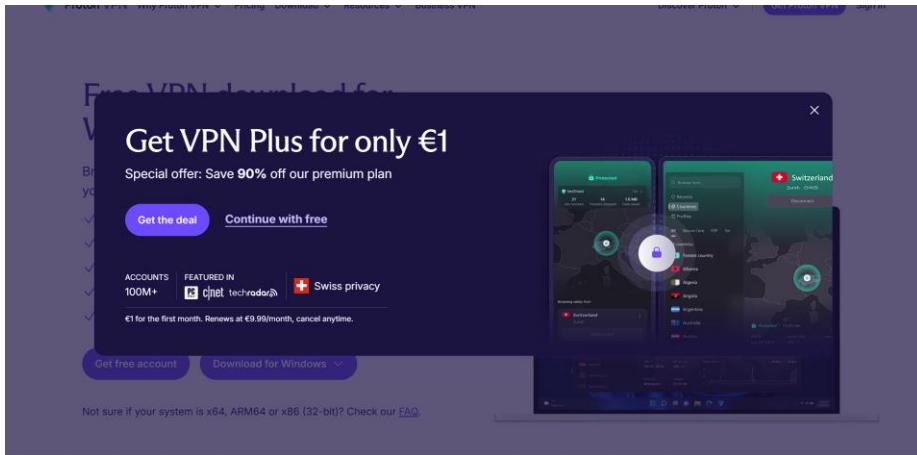
#### ❖ Tools Used

- **VPN Client:** ProtonVPN (Free Tier)
- **IP Verification Tool:** [WhatIsMyIPAddress.com](http://WhatIsMyIPAddress.com)
- **Web Browser:** Google Chrome

#### Steps Performed

##### Step 1: Selection and Download of VPN

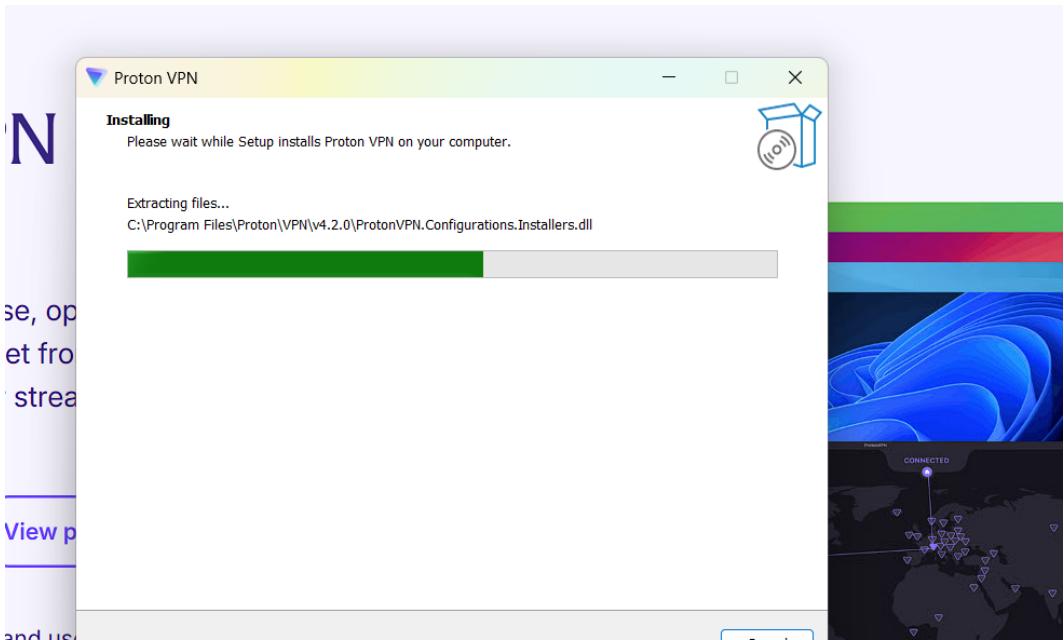
I selected **ProtonVPN (Free Tier)** for this task due to its reputable privacy policy, open-source applications, and strong security protocols. The VPN client was downloaded from the official [ProtonVPN website](http://ProtonVPN website).



A screenshot of the ProtonVPN website. The main heading is "Download VPN apps for any device". Below it, a paragraph states: "Proton VPN apps are easy to use, open source, and audited for security. Protect your internet from hackers and surveillance while accessing or streaming content anywhere in the world." Two buttons are present: "Download for Windows" and "View plans". A note below the paragraph says: "Founded by MIT and CERN scientists and used by journalists and activists all over the world, Proton VPN is working to make online privacy and security available to all." To the right, there's a large image of a computer monitor displaying a world map with various connection points, overlaid with colorful, abstract shapes.

## Step 2: Installation

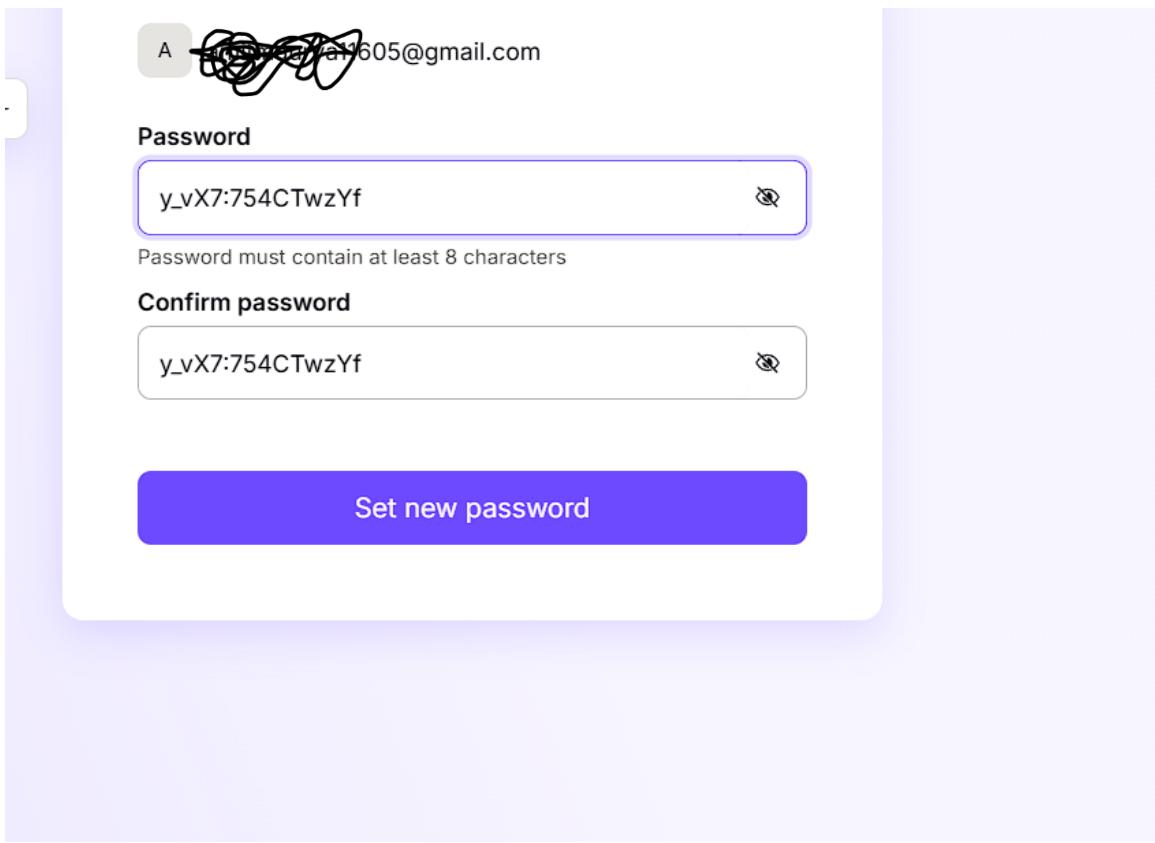
The ProtonVPN setup file was installed successfully on the system. The installation process was straightforward, with no additional software or permissions requested outside the VPN functionality.



---

### Step 3: VPN Account Setup

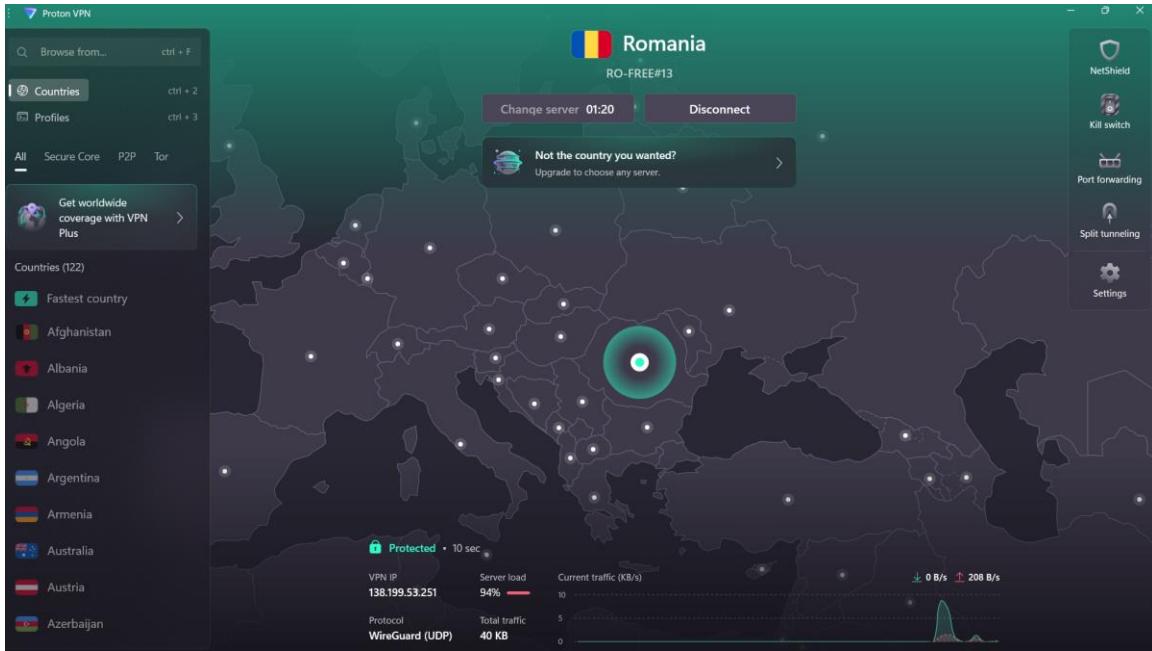
I created a **ProtonVPN free account** using a secure email address. The registration process did not require any sensitive personal information.



---

#### Step 4: VPN Connection

I logged in to the ProtonVPN client and connected to the **recommended server** with optimal speed and minimal latency.



## Step 5: IP Address Verification

To verify whether the VPN was working correctly:

- I checked my IP address using [whatismyipaddress.com](https://whatismyipaddress.com) before connecting to the VPN and noted my original IP.

My IP Address is:  
IPv6: 2405:201:6020:1957:fc5a:8fe3:d69f:53f9  
IPv4: 49.36.211.146

My IP Information: Your location may be exposed!  
ISP: Reliance Jio Infocomm  
Limited  
City: Kanpur  
Region: Uttar Pradesh  
Country: India

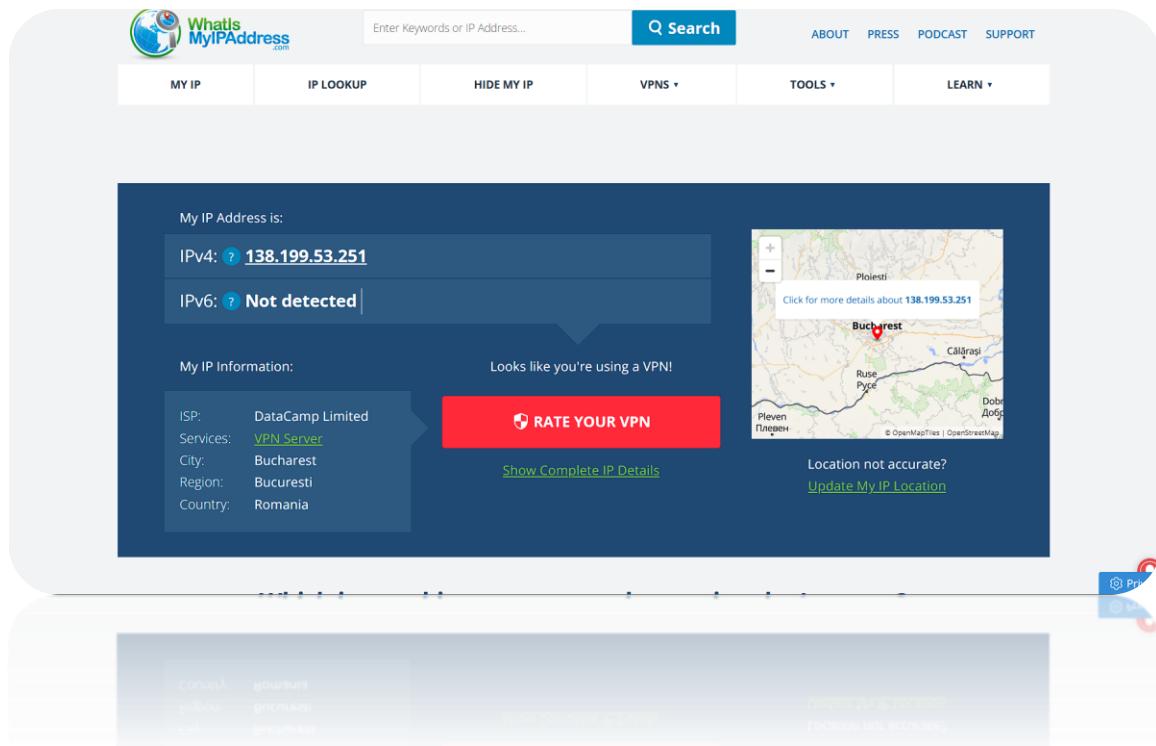
HIDE MY IP ADDRESS NOW

Click for more details about  
2405:201:6020:1957:fc5a:8fe3:d69f:53f9

Bahraich  
Kanpur  
Fatehpur  
Prayagraj

Location not accurate?  
Update My IP Location

- After connecting to ProtonVPN, I checked the IP address again. The IP address was successfully changed, confirming that my traffic was now being routed through the VPN server.



## Step 6: Secure Browsing Confirmation

I visited multiple websites and noticed the browsing experience was seamless. The VPN connection successfully encrypted my traffic and prevented direct exposure of my original IP address.

## Step 7: VPN Disconnection and Speed Comparison

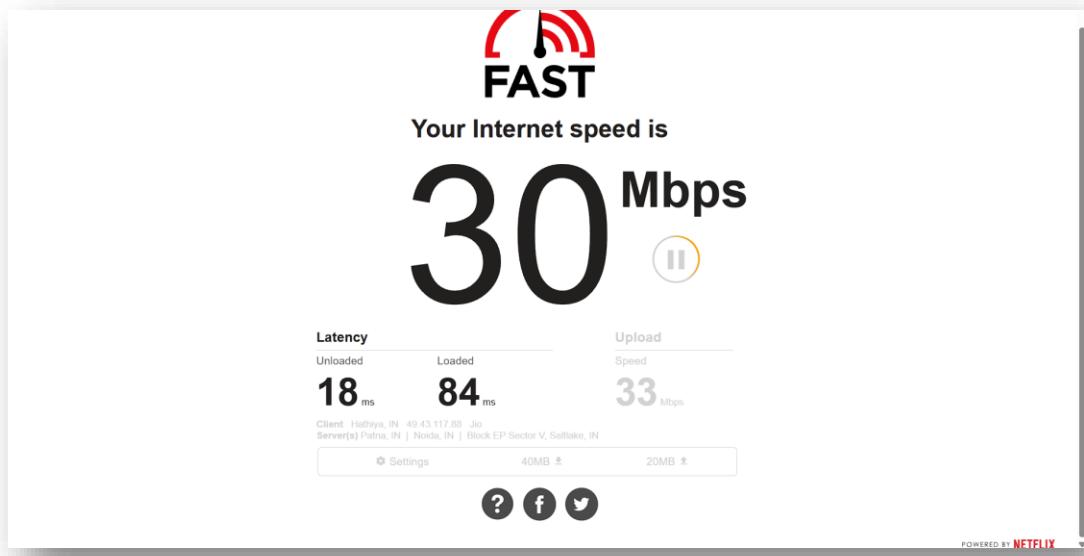
After disconnecting from the VPN:

- My IP address reverted to the original, confirming the VPN session was properly terminated.
- Browsing speed improved slightly after disconnection, which is typical as VPN encryption adds a small overhead.

- SPEED DURING VPN CONNECTION



- AFTER TERMINATING VPN CONNECTION



---

## Step 8: Research on VPN Encryption and Privacy Features

ProtonVPN uses strong encryption protocols such as:

- **AES-256 encryption** to protect data traffic.

- **OpenVPN and IKEv2/IPSec protocols** for secure tunneling.
  - **No-logs policy**, ensuring that user activity is not stored.
  - DNS leak protection and kill switch features for enhanced security.
- 

## **VPN Benefits and Limitations**

### **Benefits:**

- **Privacy Protection:** Hides real IP address and encrypts browsing activity.
- **Secure Data Transmission:** Strong encryption protocols protect sensitive information.
- **Access to Geo-Restricted Content:** Allows access to content unavailable in the user's region.
- **Public Wi-Fi Protection:** Shields traffic on insecure networks.

### **Limitations:**

- **Potential Speed Reduction:** VPN encryption can reduce browsing speed.
- **Limited Servers in Free Plans:** Free VPNs often have limited server access and bandwidth.
- **Not Fully Anonymous:** VPNs mask IPs but do not guarantee complete anonymity.
- **Dependence on VPN Provider Trust:** User security is only as strong as the provider's privacy practices.