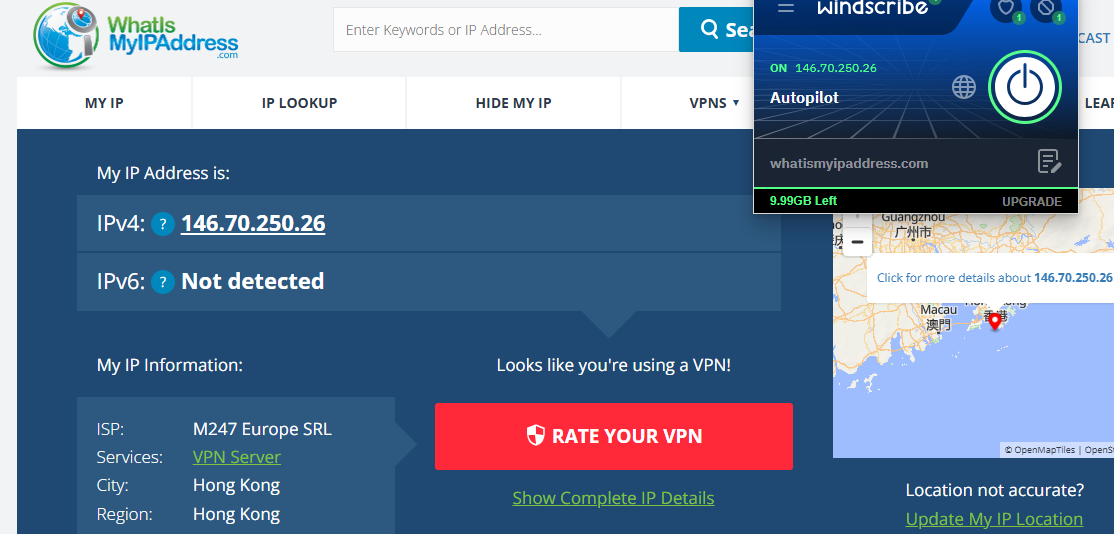
ELEVATE LABS Harshitha M

TASK 8 Report:

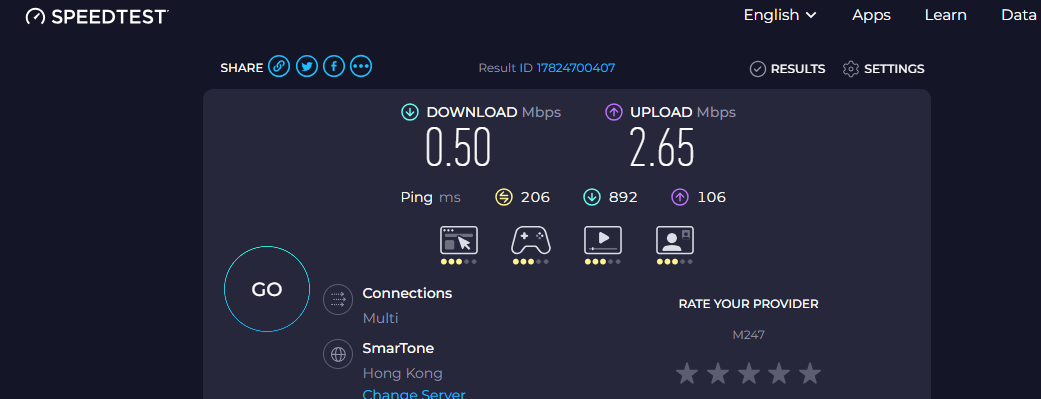
Setting up of VPN using Microsoft Edge extension

1. Choose the free VPNs available,here I used windscribe vpn
2. It can be downloaded or can be used through browser
3. Here I have downloaded the extension of Edge browser
4. Next, create an account and autopilot is turned on
5. The browser is connected to the VPN
6. In order to check the ip address of the system, I have used website called whatismyipaddress.com to check the location of my ip address
7. Here is the snippet of the output generated

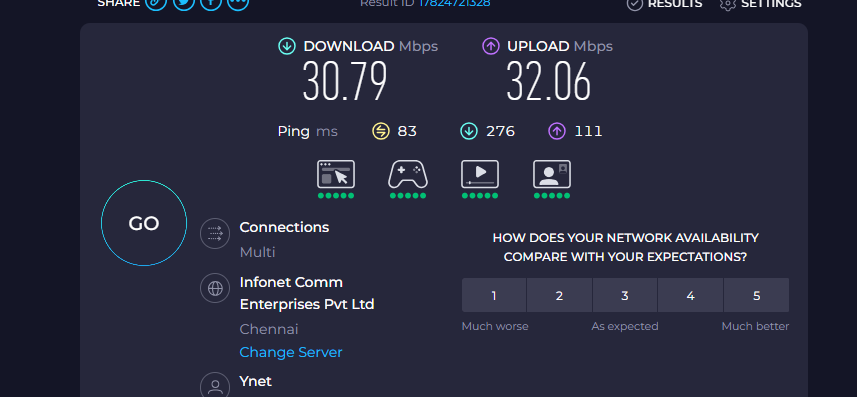




Testing the speed of the internet through this server



Testing without VPN connection



Inference

Why VPN Slows Down Internet Speed:

1. Data Encryption Overhead:
   * VPNs encrypt your data before sending it through the tunnel. This encryption and decryption process takes time and consumes processing power.
2. Longer Routing Path:
   * Your internet traffic is routed through the VPN server (which could be in a different country), adding distance and delay (increased latency).
3. Server Load:
   * If many people are using the same VPN server, it can become overloaded, leading to slower speeds.
4. VPN Protocol Used:
   * Different protocols (like OpenVPN, IKEv2, WireGuard) offer different balances of speed and security. Some are slower due to stronger encryption.
5. ISP Throttling (sometimes reversed):
   * Without VPN, your ISP may offer full speed. But some ISPs throttle VPN traffic, or VPN may bypass other throttling depending on the case.

Windscribe VPN: Encryption & Privacy Features

✅ 1. Encryption Standards

* Encryption Type: AES-256 (Advanced Encryption Standard – 256-bit)
* Handshake Encryption: RSA-4096
* Data Authentication: SHA-512

This is military-grade encryption, considered very secure and widely used by top-tier VPNs.

2. VPN Protocols Supported

Windscribe offers a variety of VPN protocols for flexibility in speed and security:

| Protocol | Description | Speed | Security |
| --- | --- | --- | --- |
| WireGuard | Modern, fast, and efficient protocol | ⚡⚡⚡⚡⚡ | 🔐🔐🔐🔐 |
| OpenVPN (UDP/TCP) | Trusted open-source protocol | ⚡⚡⚡ | 🔐🔐🔐🔐🔐 |
| IKEv2/IPSec | Great for mobile devices | ⚡⚡⚡⚡ | 🔐🔐🔐🔐 |
| Stealth Protocol | Obfuscates VPN traffic (bypasses firewalls and censorship) | ⚡⚡ | 🔐🔐🔐🔐 |

💡 You can choose protocols manually or let Windscribe auto-select based on performance.

3. Logging & Privacy Policy

Windscribe has a strong no-logs policy, meaning:

* ❌ No storing of your IP address, browsing activity, or connection timestamps
* ✅ Temporarily logs bandwidth usage to enforce free plan limits
* ✅ Clearly documented privacy policy and transparent company practices

Location: Based in Canada (5 Eyes Alliance member) — however, their infrastructure and zero-logs stance help mitigate surveillance risks.

4. DNS, Leak & IP Protection

Windscribe includes strong privacy protections:

* ✅ Custom DNS servers to prevent DNS leaks
* ✅ IPv6 Leak Protection
* ✅ WebRTC Leak Protection
* ✅ Kill Switch (Firewall) to cut off all internet if the VPN drops (prevents real IP leaks)

5. Extra Privacy Features

* 🧅 "Double Hop" feature: Route traffic through two different VPN servers for added anonymity
* 🧽 "R.O.B.E.R.T.": A customizable DNS-level blocker that filters ads, trackers, malware, and even specific content categories (like gambling or fake news)

**Benefits of Using a VPN**

1. **Privacy Protection**
   * Hides your IP address from websites, apps, and services.
   * Prevents ISPs and third parties from tracking your online activities.
2. **Secure Data Transmission**
   * Encrypts internet traffic, protecting data on public Wi-Fi or unsecured networks.
   * Useful when working remotely or accessing sensitive data.
3. **Access Geo-Restricted Content**
   * Allows you to bypass content restrictions and censorship (e.g., Netflix, Hulu, YouTube).
   * Helps access blocked websites in countries with strict internet regulations.
4. **Avoid Bandwidth Throttling**
   * ISPs sometimes slow down speeds for certain activities (e.g., streaming); VPNs can mask this behavior.
5. **Remote Access to Networks**
   * Useful for businesses allowing employees to securely connect to company networks from anywhere.

**❌ Limitations of Using a VPN**

1. **Reduced Internet Speed**
   * Encryption and rerouting traffic can slow down connection speeds, especially on free or distant servers.
2. **No Full Anonymity**
   * VPN hides your IP but doesn't protect against all tracking methods (cookies, browser fingerprinting, etc.).
3. **Not a Complete Security Solution**
   * Doesn't block malware or phishing sites by default (unless combined with antivirus or ad-blockers).
4. **Some Services Block VPNs**
   * Websites (like streaming platforms or banks) may detect and block VPN traffic.
5. **Trust in VPN Provider**
   * You’re shifting trust from your ISP to the VPN provider—some may log your data or have weak privacy policies.
6. **Legal and Policy Risks**
   * VPN use is restricted or illegal in some countries (e.g., China, Iran, UAE).