**Task 8: Working and understanding VPN**

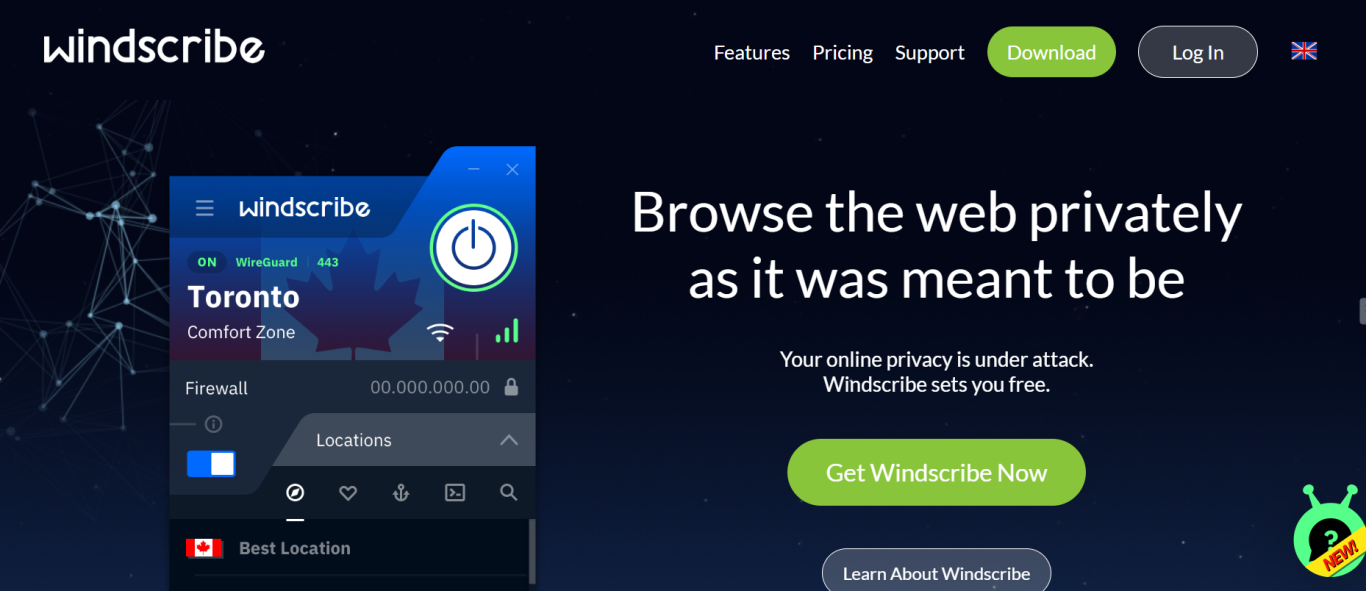
**Objective:** Understand the role of VPNs in protecting privacy and secure communication.

**Tools:** Free VPN client (ProtonVPN free tier, Windscribe free)

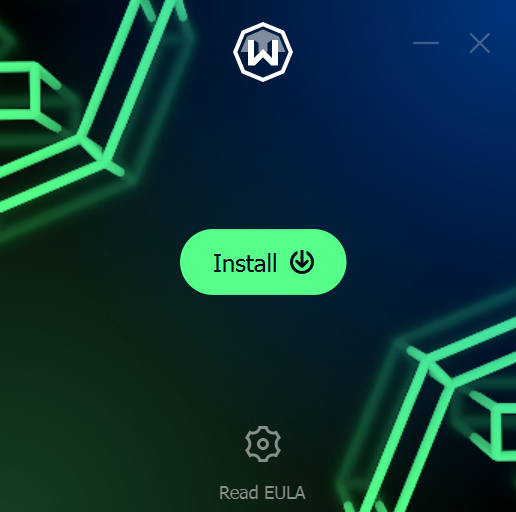
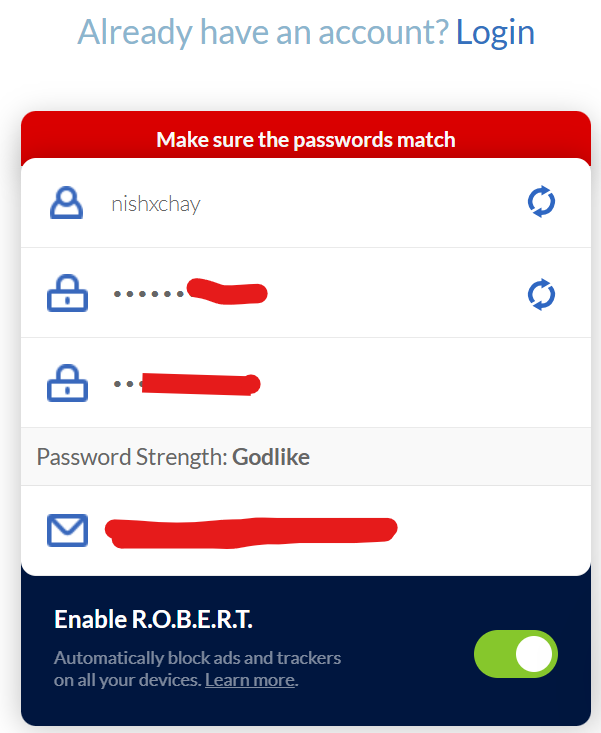
**Deliverables:** Report describing VPN setup steps and connection status screenshot.

1. **Choose a reputable free VPN service and sign up.**

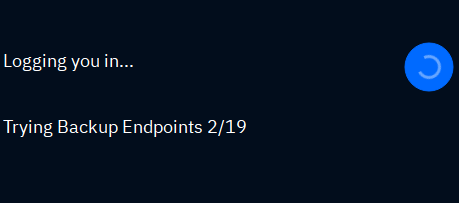
Here for our working, we chose **“Windscribe”**.

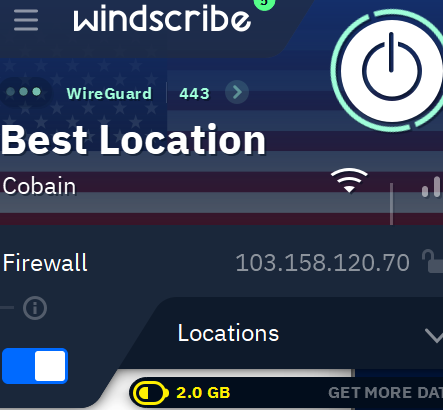
****

1. **Download and install the VPN client.**



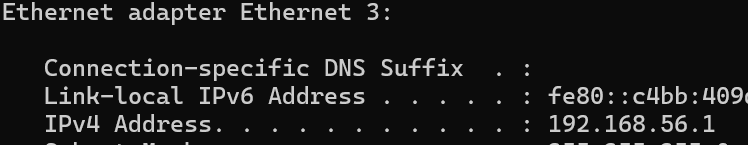
1. **Connect to a VPN server (choose closest or any location).**

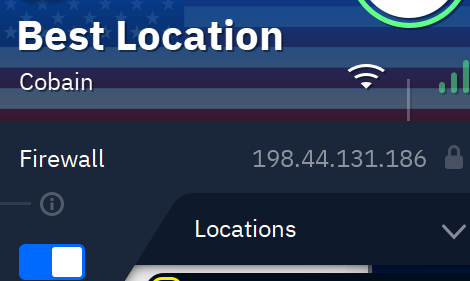




Here, we chose UNITED STATES.

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

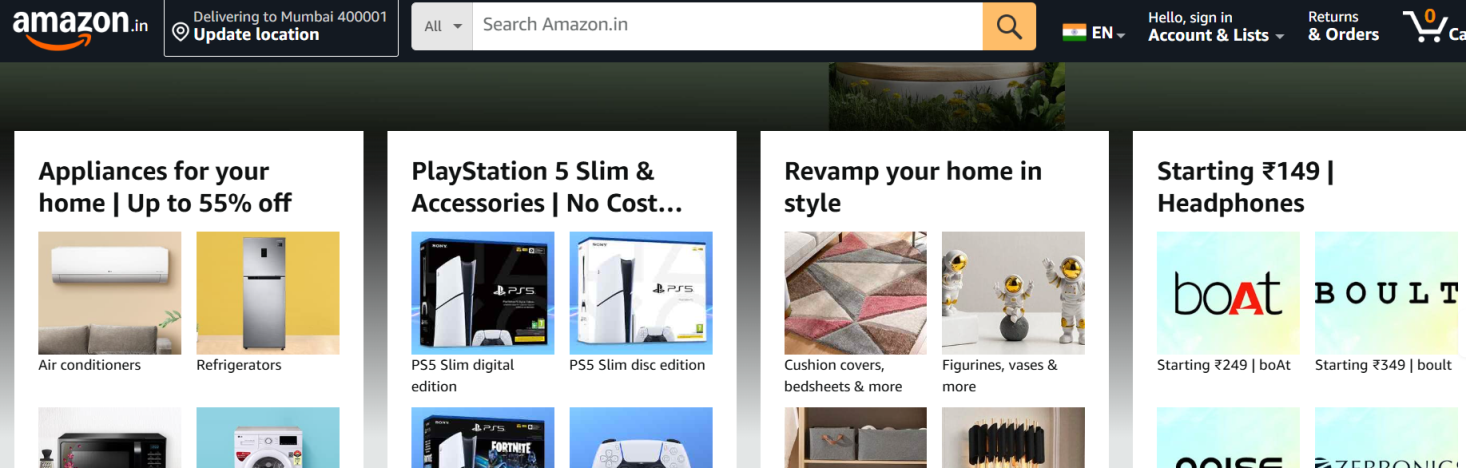






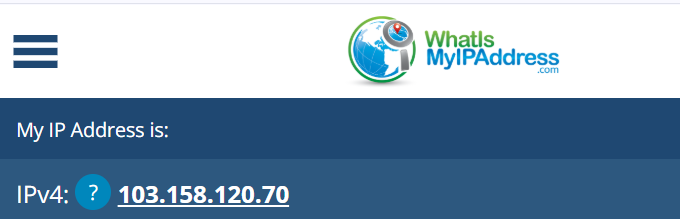
So, IP Address has been changed.

1. **Browse a website to confirm traffic is encrypted.**



Yes, traffic is encrypted.

1. **Disconnect VPN and compare browsing speed and IP.**



**IP:** IP address changes.

**Browsing Speed :** VPNs work by encrypting your internet traffic and routing it through a remote server. This process can add a slight delay (latency) and potentially reduce your browsing speed, [according to Fortinet](https://www.fortinet.com/resources/cyberglossary/does-vpn-decrease-internet-speed).

Turning off a VPN resulted in a **faster browsing speed**, as the encryption and routing through a remote server no longer added latency.

However, the speed increase is usually **not drastic**, and might only be noticeable during **specific tasks** like **streaming/downloading** large files.

1. **Research VPN encryption and privacy features.**

VPN encryption and privacy features work together to secure your online data and activity. VPNs create encrypted tunnels, or virtual connections, that protect your data from unauthorized access while also concealing your IP address and masking your virtual location.

**Encryption:**

* **Data Encryption:**

VPNs use encryption to scramble your data, making it unreadable to anyone who might try to intercept it, including hackers, cybercriminals, or even your internet service provider.

* **Protocols:**

Different VPN providers use various encryption protocols, like OpenVPN, IPsec, and L2TP/IPsec.

* **No-Logs Policy:**

A no-logs policy, where the VPN provider doesn't keep records of your online activities, further enhances privacy by ensuring your browsing history remains hidden.

**Privacy Features:**

* **IP Address Masking:**

VPNs redirect your internet traffic through a remote server, assigning you a new IP address, effectively hiding your real IP from websites and services.

* **Virtual Location:**

You can choose a VPN server location to make it appear as if you're browsing from that location.

* **Anonymization:**

VPNs help anonymize your online activity by masking your identity and location.

1. **Write a summary on VPN benefits and limitations.**

Benefits:

* **Enhanced Privacy:**

VPNs encrypt your internet traffic and hide your IP address, making it harder for third parties to track your online activity and location.

* **Secure Public Wi-Fi:**

They provide a secure connection when using public Wi-Fi hotspots, protecting your data from eavesdropping.

* **Bypassing Geo-blocks:**

VPNs can help you access geo-blocked content and services by making your connection appear to be from a different location.

* **Protection from Cyberattacks:**

VPNs can help protect against certain types of cyberattacks, such as DDoS and man-in-the-middle attacks.

* **Secure Remote Work:**

They enable secure and encrypted access to company networks and resources when working remotely.

Limitations:

* **Slower Speeds:** Encryption and rerouting traffic through VPN servers can slightly reduce internet speeds.
* **Subscription Costs:** Most VPN services require a subscription fee.
* **Not a Silver Bullet:** VPNs are not a replacement for antivirus software or other security measures.
* **Potential Data Leaks:** The security of a VPN depends on the provider's practices, and some VPNs may leak IP addresses or log data.
* **Geo-blocking Issues:** Some services may still detect and block VPN connections.
* **Not Always Compatible:** VPNs might not be compatible with all devices or older systems.
* **Data Limits with Free VPNs:** Free VPNs often impose data limits, restrict bandwidth, and offer limited server options.