Task – 8 Working and Understanding VPN

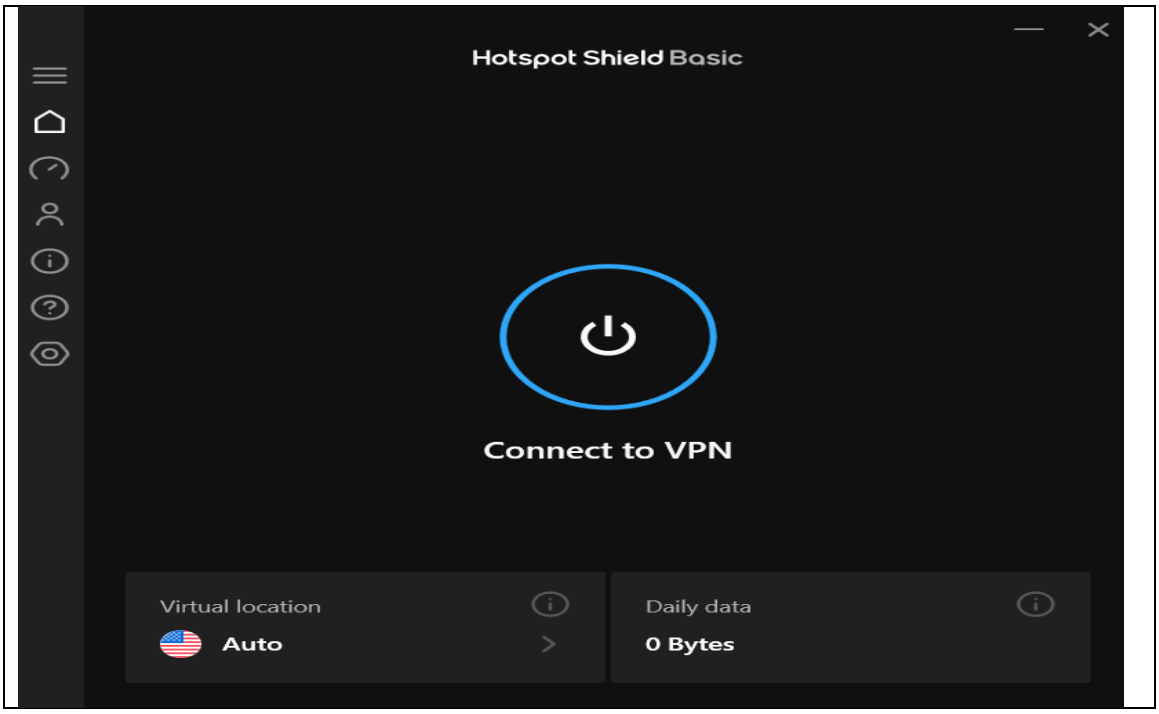
Objective: Understand the role of VPNs in protecting privacy and secure communication.
Tools: Free VPN client (Hotspot Shield VPN or any other VPN Service.)

STEPS TAKEN:

1. **The first step is to install any VPN service of your choice.**
   In my case, **Hotspot Shield VPN** is already pre-installed, so I do not need to install it again. However, if you do not have a VPN installed, it is recommended that you register on the respective website and download the VPN client to proceed with further steps.
   In my case: https://www.hotspotshield.com/vpn

2. **Install and Launch Hotspot Shield VPN**

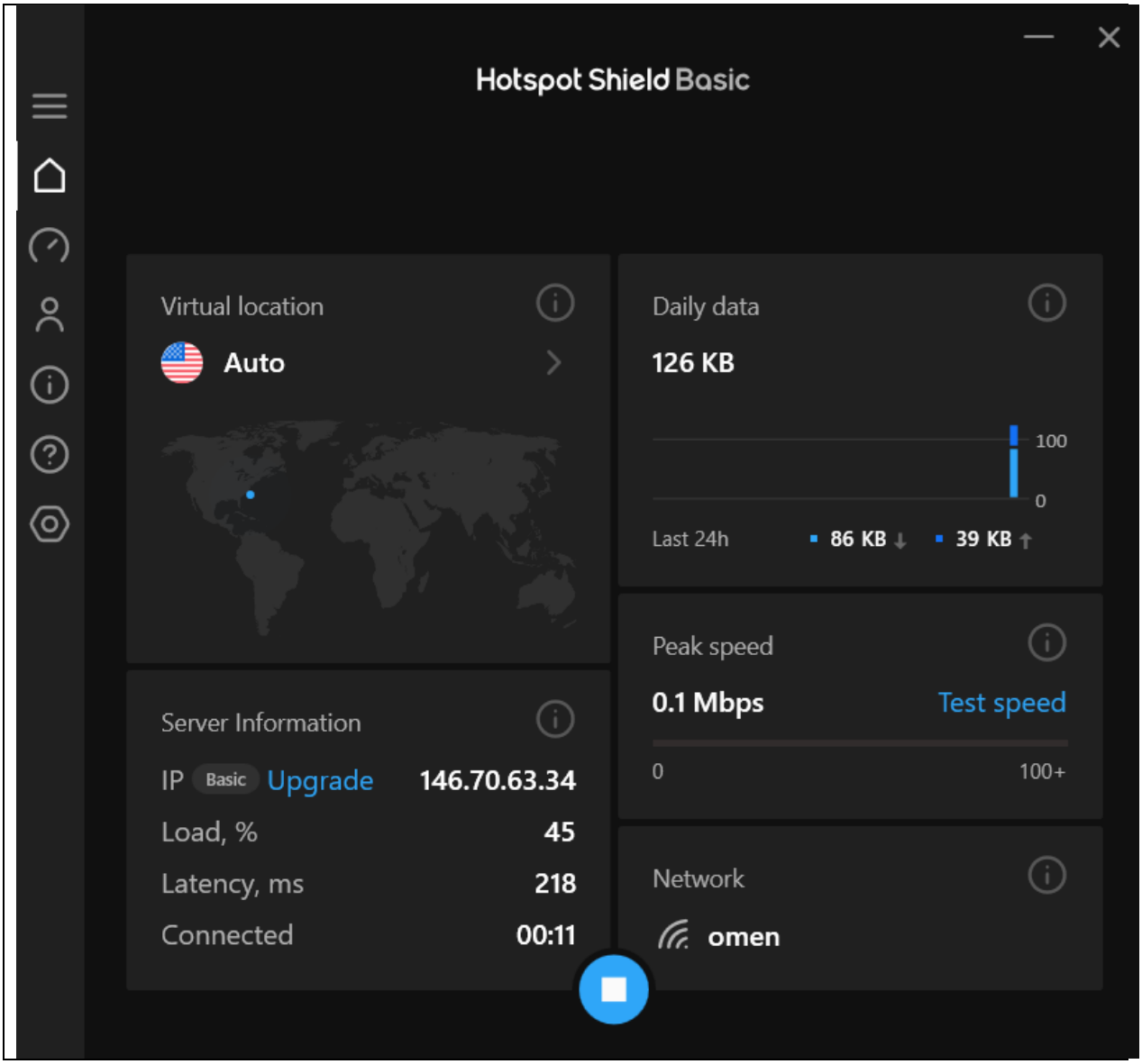
- Install the downloaded setup file using the default installation settings.
- Launch the Hotspot Shield application after installation is complete.



3. Click the **“Connect to VPN”** button in the Hotspot Shield app.

   The app will automatically connect to the fastest available free server (usually a U.S. location).

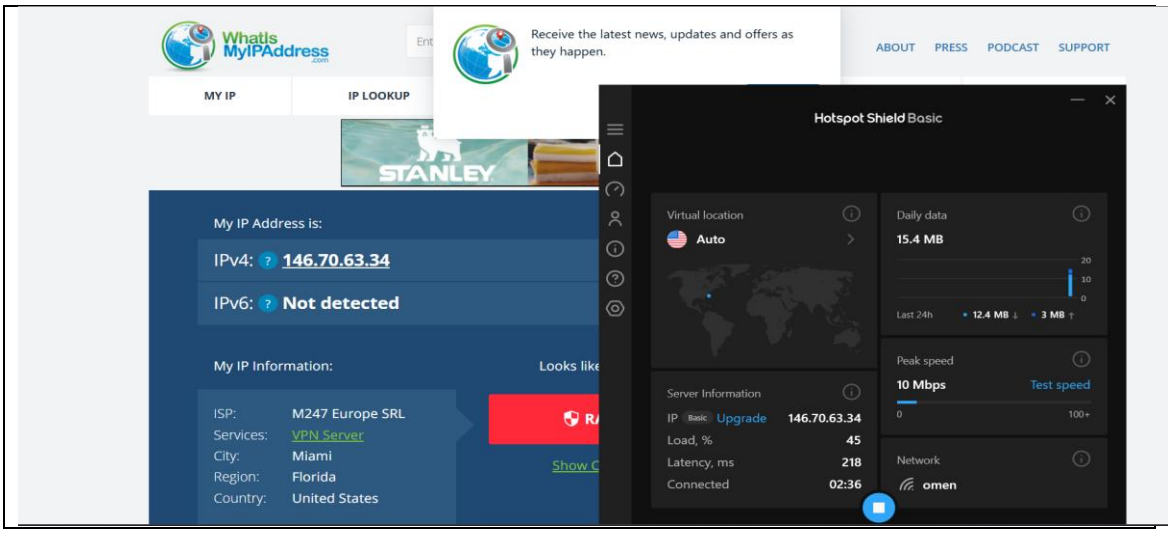
   After connecting successfully;



In Hotspot Shield VPN it has several features as it shows the new IP address and the speed of the internet in the client itself.

But still we can check it online for the real IP address.

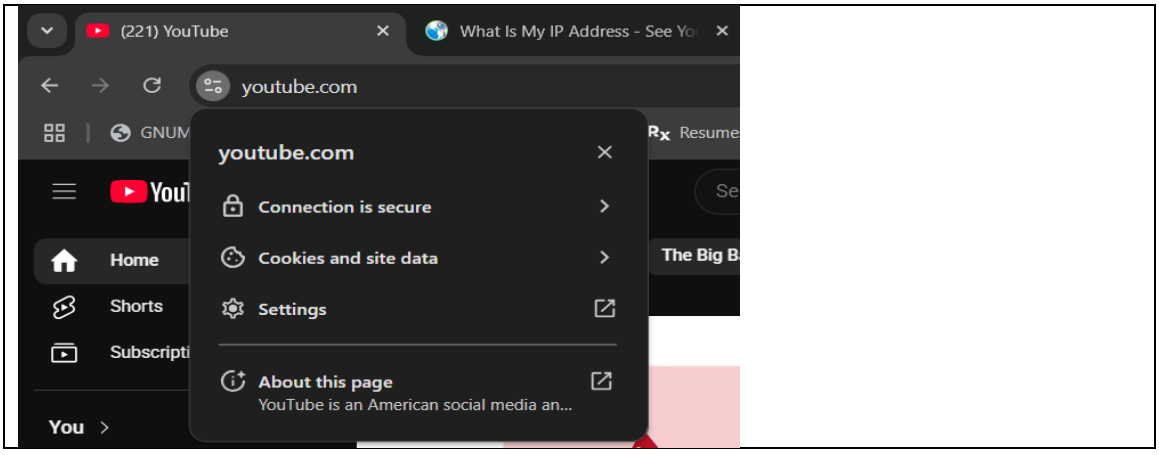
4. Now checking the IP address using online website like https://whatismyipaddress.com which can help you to know the exact IP address of yours.



Here, we can clearly see that the IP address allocated by the VPN client matches the IP address shown on the website.

5. **Confirming Encrypted Traffic**

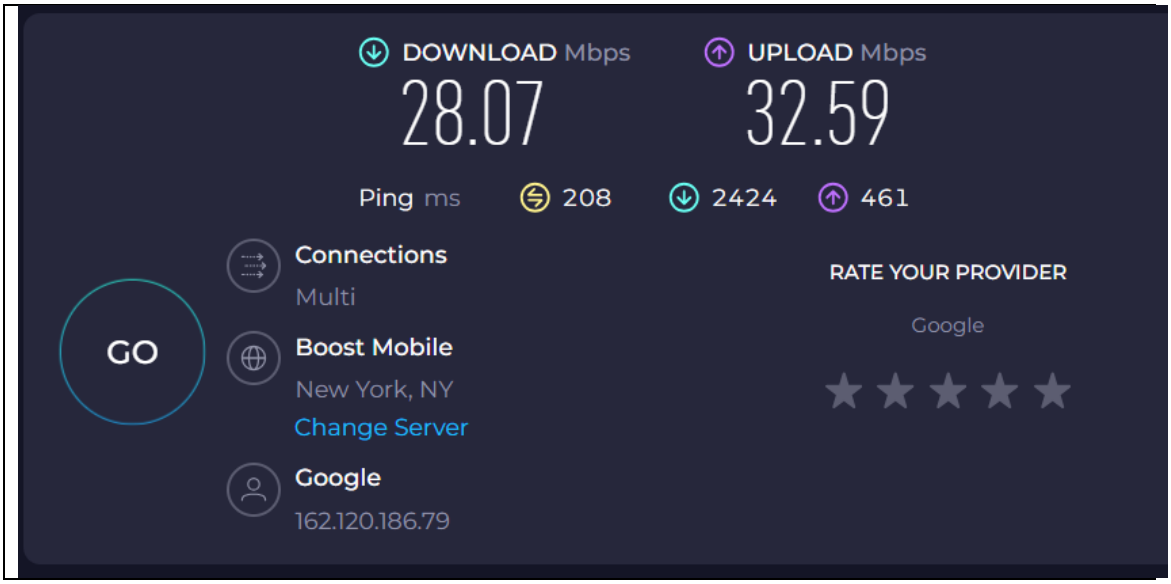
- Open a secure website (e.g., https://youtube.com) while connected to the VPN.
- Ensure the website uses HTTPS (indicated by a padlock icon in the address bar).
- Verify that browsing works normally and securely.



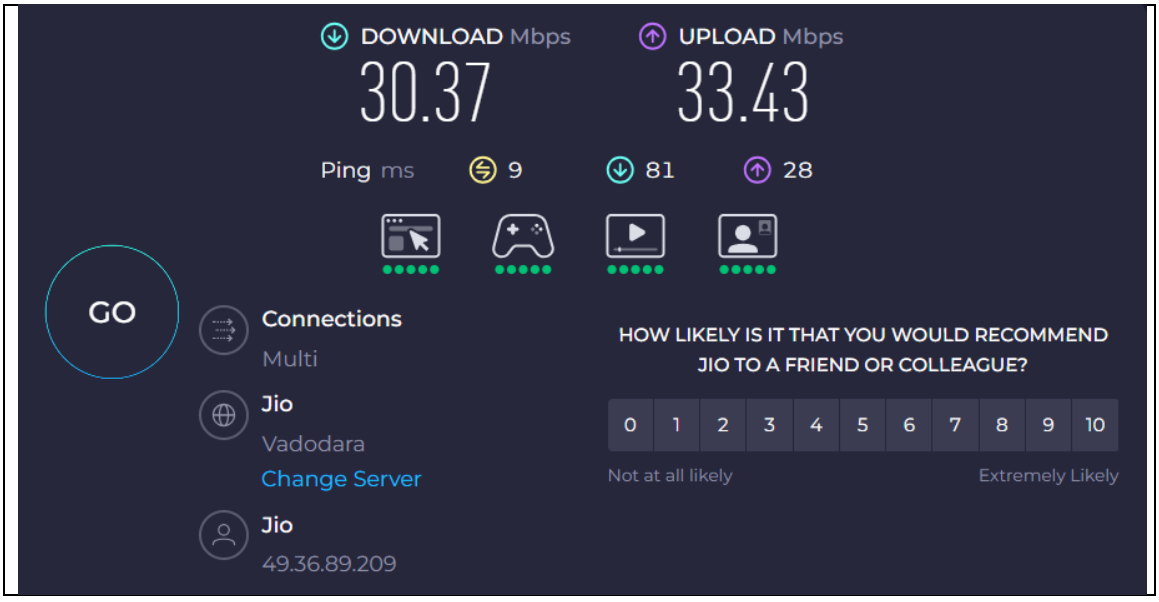
6. Disconnect from the VPN by clicking the **“Stop”** or **“Disconnect”** button.

   Check your browsing speed before and after using the VPN.

   This is speed of Internet while are I was connected to VPN.



   This is speed of internet after I disconnected my VPN.



VPN Encryption and Privacy Features

A **Virtual Private Network (VPN)** creates a secure, encrypted connection—also known as a "tunnel"—between your device and the internet. This encryption ensures that your online data is protected from unauthorized access, even on untrusted networks like public Wi-Fi.

Key Encryption and Privacy Features:

- **Encryption Protocols:** VPNs use protocols like **OpenVPN**, **IKEv2/IPSec**, **WireGuard**, and **L2TP/IPSec** to encrypt data. These protocols determine how secure and fast the VPN connection is.
- **End-to-End Encryption:** Data is encrypted on your device and decrypted only once it reaches the VPN server, protecting your activity from ISPs, hackers, and local networks.
- **IP Address Masking:** VPNs replace your real IP address with that of the VPN server, hiding your location and making your online identity more anonymous.
- **No-Log Policies:** Many reputable VPN services commit to **not storing logs** of your activity, enhancing privacy (though this depends on the provider's trustworthiness and jurisdiction).
- **Kill Switch:** This feature automatically disconnects your internet if the VPN connection drops, preventing accidental data leaks.
- **DNS Leak Protection:** Prevents your DNS queries from being exposed outside the VPN tunnel, ensuring complete privacy.

VPN Benefits

1. **Improved Online Privacy:** Hides your IP and encrypts your data, making it harder for websites, ISPs, and attackers to track your activity.
2. **Secure Public Wi-Fi Usage:** Protects your data from being intercepted on unsecured networks like cafés, airports, etc.
3. **Bypass Censorship and Geo-blocks:** Access content restricted in your region, including websites, streaming services, and apps.
4. **Protection from ISP Throttling:** Prevents ISPs from seeing your activity, which can stop them from slowing down your connection based on usage.
5. **Remote Access:** Enables employees to securely connect to corporate networks from anywhere.

VPN Limitations

1. **Trust in VPN Provider:** Your data is visible to the VPN server, so privacy depends on the provider's honesty and jurisdiction.
2. **Reduced Speed:** Encryption and routing slightly **slows down your internet speed**, especially with distant servers.
3. **Not a Complete Anonymity Tool:** VPNs don't prevent browser fingerprinting, tracking cookies, or malware—additional tools are needed.
4. **Legality and Policy Restrictions:** Some countries ban or limit VPN use; violating terms of service can lead to service bans.
5. **Cost:** High-quality VPNs are usually subscription-based; free ones may compromise your privacy or include ads.