Objective

To understand how Virtual Private Networks (VPNs) function by setting up a free VPN, verifying encrypted traffic, analyzing IP masking, and researching encryption and privacy features.

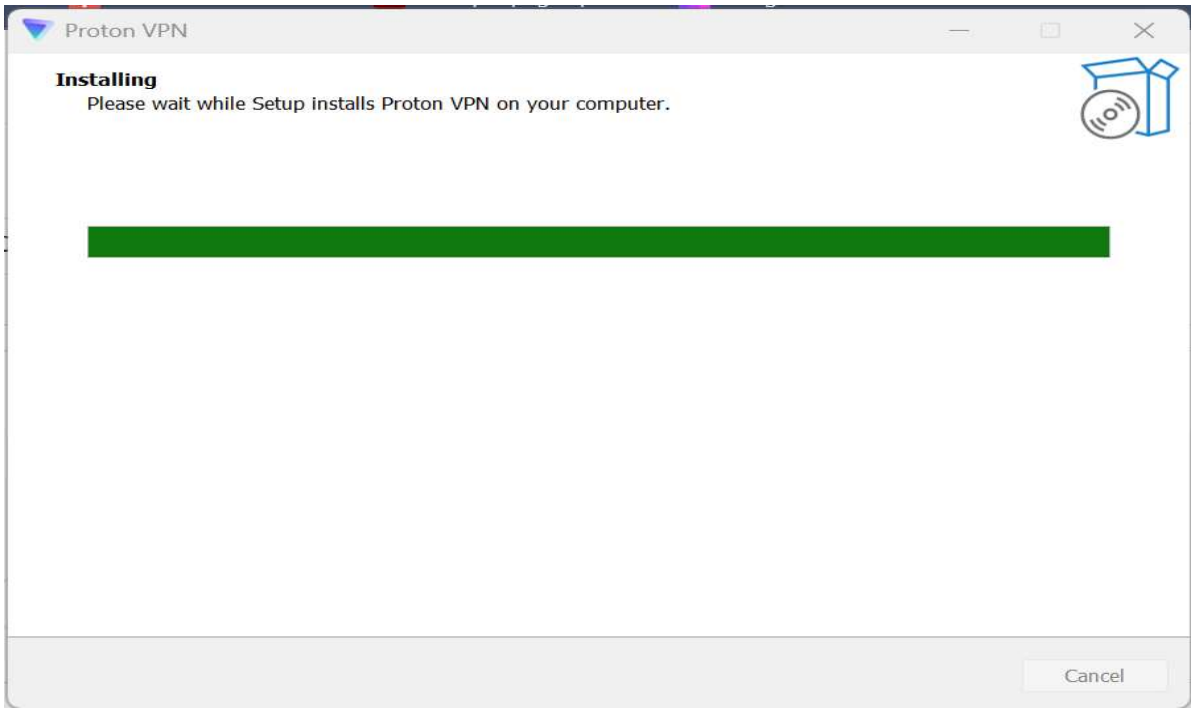
Steps Performed

Step 1 – VPN Selection and Account Creation

- **VPN Chosen**: ProtonVPN (Free Plan)
- Signed up via https://protonvpn.com/free-vpn

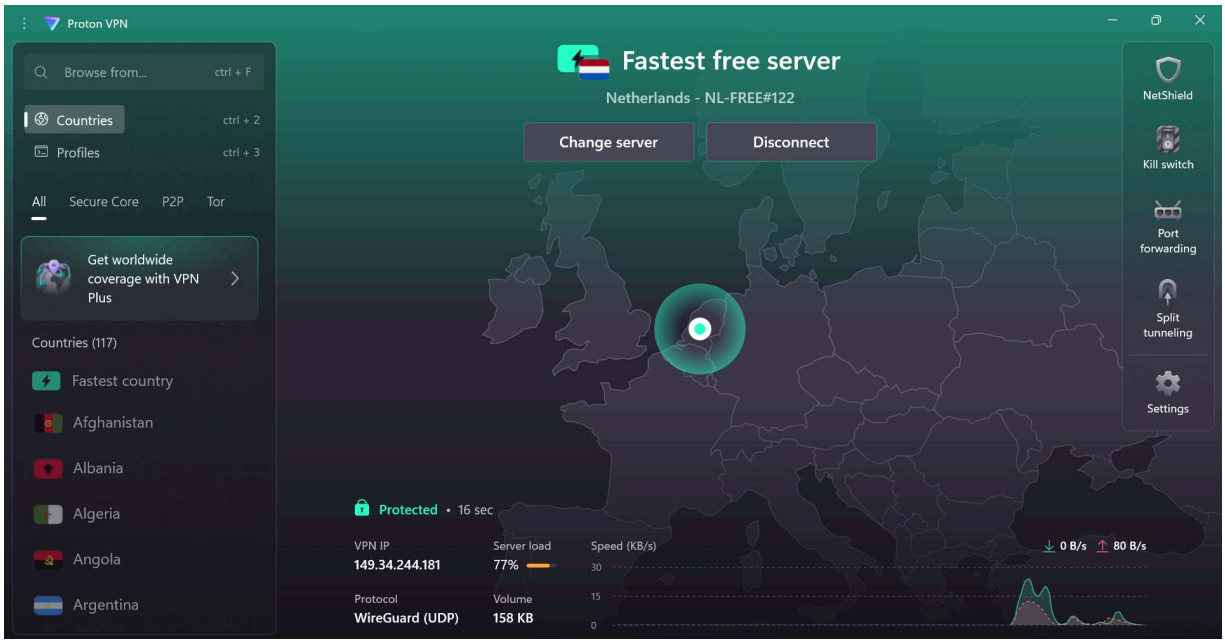
Step 2 – Download and Installation

- Installed ProtonVPN client on Windows.



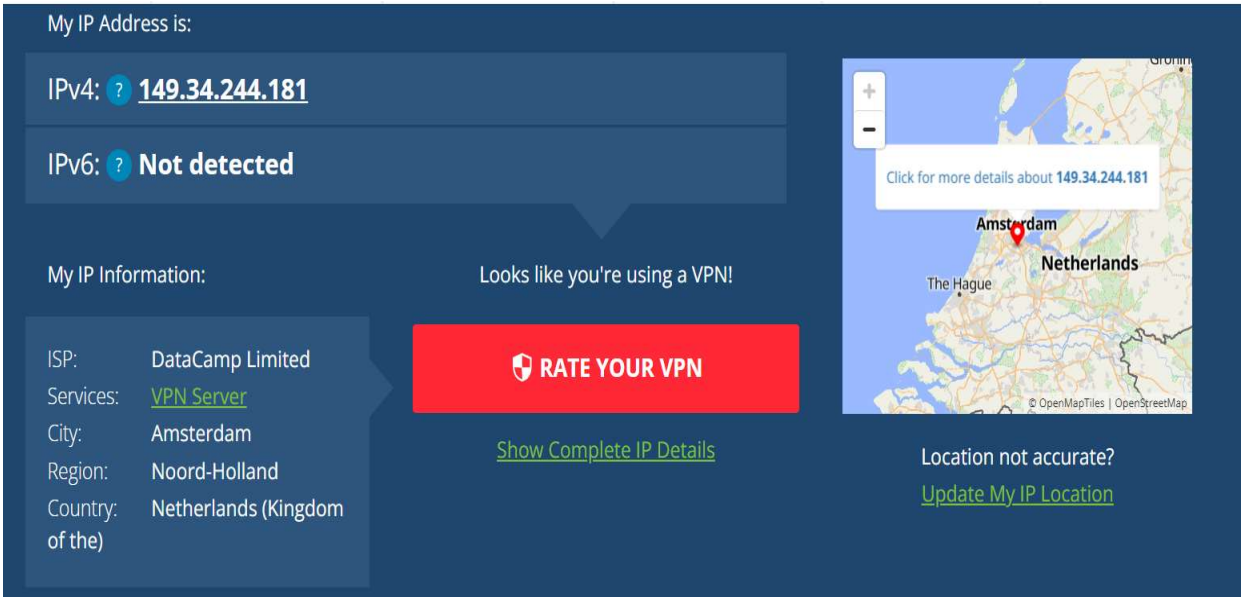
Step 3 – Connecting to a VPN Server

- Connected to a nearby server (e.g., India or Netherlands)



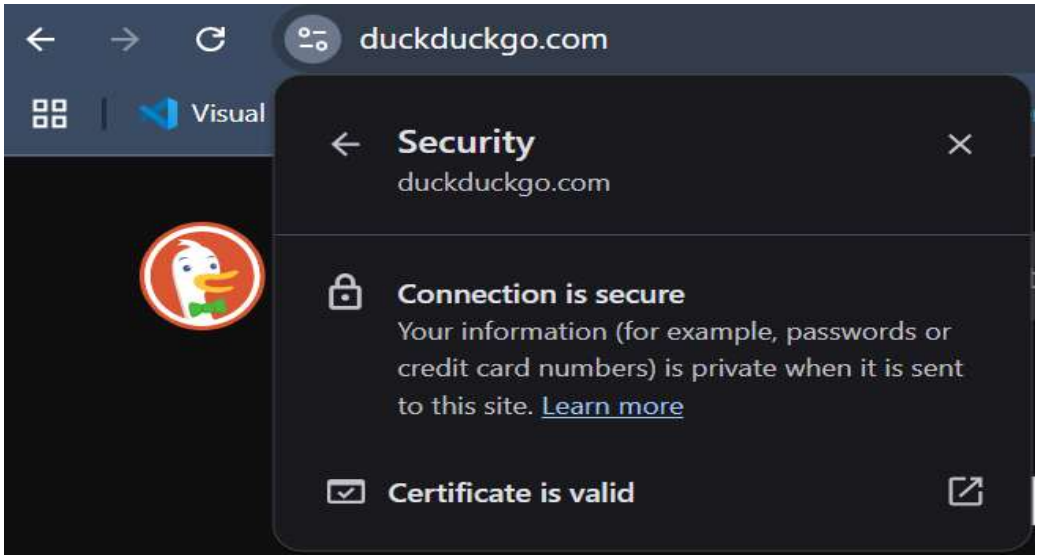
Step 4 – Verifying IP Address

- Visited https://whatismyipaddress.com
- Noted masked IP address and changed location



Step 5 – Confirming Encrypted Traffic

- Visited HTTPS-enabled website (e.g., duckduckgo.com)
- Checked browser lock icon and certificate info



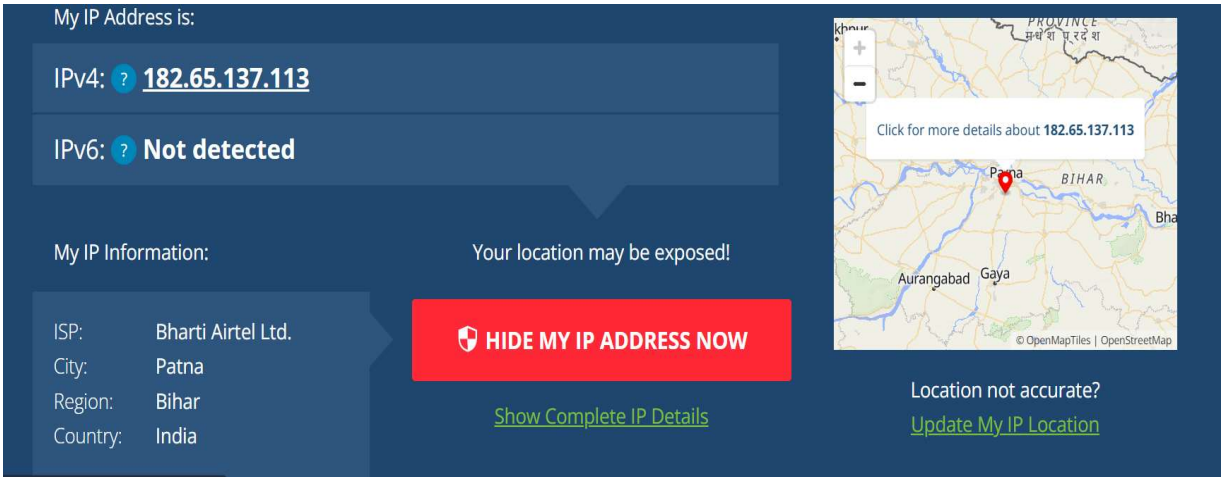
I accessed https://duckduckgo.com with and without the VPN enabled. In both cases, the browser showed a secure HTTPS connection, indicating end-to-end encryption between the browser and the website.

However, with the VPN active, all traffic — including DNS requests and non-browser data — was encrypted and tunneled through the VPN server. This offers broader protection by hiding browsing activity from the ISP and securing all outbound traffic, not just browser-based HTTPS sessions.

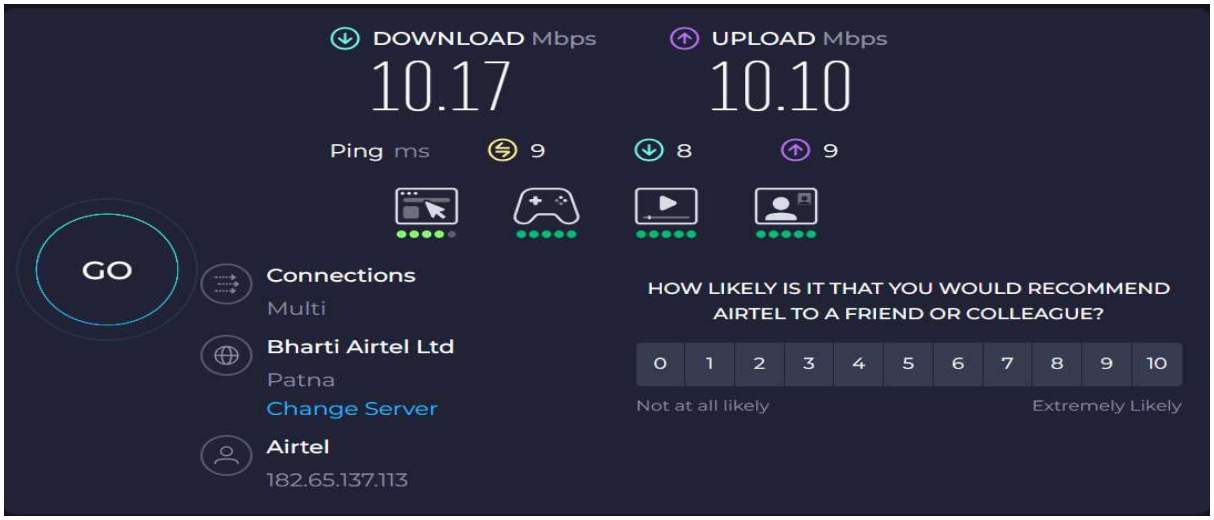
This step highlighted the difference between site-specific encryption (**HTTPS**) and network-level encryption (**VPN**), both essential for comprehensive data security.

Step 6 – Disconnect and Compare

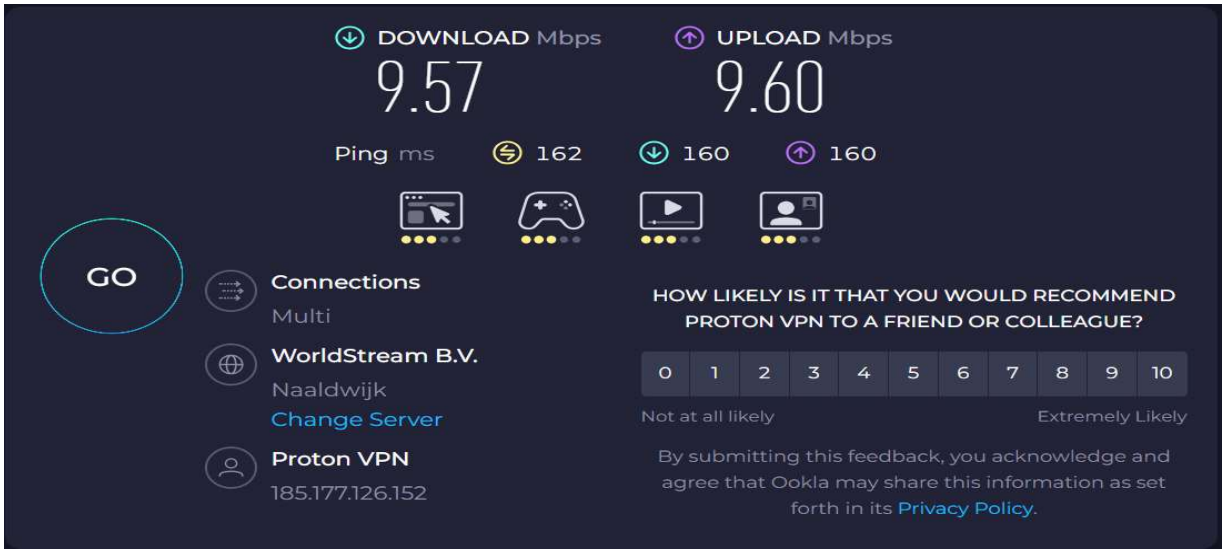
- Disconnected VPN and rechecked IP address
- Compared speed and noted original location restored



Speed Test without VPN:



Speed Test with VPN:



Research: VPN Encryption and Privacy Features

Virtual Private Networks (VPNs) function by creating an encrypted tunnel between the user's device and a remote server, masking IP addresses and securing data from potential interception. The level of security a VPN offers depends largely on the encryption protocols and privacy mechanisms it implements.

Encryption Standards :

Most modern VPNs use AES-256 (Advanced Encryption Standard) encryption — a symmetric key cipher widely regarded as secure and virtually unbreakable through brute force. This standard is used by governments, militaries, and financial institutions worldwide.

VPNs typically implement encryption using protocols such as:

- OpenVPN: Open-source, reliable, and supports strong cryptographic algorithms.
- WireGuard: A newer protocol designed for speed, simplicity, and strong modern cryptography (e.g., ChaCha20 for encryption, Poly1305 for authentication).
- IKEv2/IPSec: Efficient on mobile devices due to seamless reconnection during network switches (Wi-Fi to cellular).

Privacy Protection Features :

Reputable VPNs offer several features to uphold user privacy:

- No-Logs Policy: Ensures the provider does not store data on user activities, browsing history, or connection times. This is essential for anonymity.
- DNS Leak Protection: Prevents requests from being resolved by external DNS servers, which could expose browsing activity.
- Kill Switch: Immediately blocks all internet traffic if the VPN connection drops unexpectedly, preventing accidental data leaks.
- Shared IP Addresses: Multiple users share a single IP, making it difficult to associate activity with a specific individual.
- Obfuscation/Stealth Modes: Some VPNs can hide the fact that VPN usage is occurring, useful in countries or networks that block VPN traffic.

Overall, VPNs with strong encryption protocols and robust privacy policies are an essential tool for secure internet usage, particularly on untrusted networks like public Wi-Fi.

Summary: VPN Benefits and Limitations

Through this task, I tested a free VPN (ProtonVPN) to understand its practical impact on privacy and internet security. Upon connection, my IP address was successfully masked, and encrypted browsing was confirmed using HTTPS sites and public IP check tools.

Benefits of VPNs:

- **Enhanced Online Privacy**: Hides real IP address, preventing websites and ISPs from tracking user location or identity.
- **Encrypted Data Transmission**: Protects sensitive information from eavesdroppers, especially on unsecured networks.
- **Bypassing Geo-Restrictions**: Allows access to content restricted in certain countries or regions.
- **Public Wi-Fi Protection**: Prevents session hijacking and packet sniffing in public hotspots.

Limitations of VPNs:

- **Performance Impact**: VPN encryption can reduce internet speed, especially when connected to distant servers.
- **Free VPN Restrictions**: Limited bandwidth, slower speeds, or fewer server choices.
- **No Protection from All Threats**: VPNs don't block phishing, malware, or insecure apps by themselves.
- **Trust in the VPN Provider**: Users must trust that the VPN truly honors its no-logs policy and doesn’t collect sensitive information.

Conclusion

This VPN task helped reinforce my understanding of how encryption, IP masking, and tunneling protocols contribute to privacy and cybersecurity. By hands-on testing with ProtonVPN, I learned how to assess VPN effectiveness, verify encryption, and understand real-world usage and limitations. This knowledge is essential when evaluating secure communication systems or recommending protective measures in cybersecurity roles.