# VPN Setup and Usage Report

## 1. Introduction

A Virtual Private Network (VPN) is a technology that creates a secure and encrypted connection between a device and the internet. VPNs protect user privacy by masking the IP address and routing internet traffic through remote servers, making it difficult for third parties to monitor or track online activity.

## 2. Objective

The objective of this task was to:  
- Install and configure a free VPN.  
- Connect to a VPN server and verify the IP change.  
- Understand the benefits and limitations of VPNs.  
- Answer interview-style questions about VPNs.

## 3. Tools Used

- VPN Client: ProtonVPN (Free Tier)  
- Verification Tool: https://whatismyipaddress.com  
- Operating System: Windows 10/11

## 4. Steps Followed

- Sign Up for ProtonVPN Free Account: Created a free account on ProtonVPN’s official website and selected the free plan (no credit card required).

- Download and Install ProtonVPN Client: Downloaded the Windows version of the ProtonVPN application from the official website and installed it using default settings.

- Connect to VPN Server: Opened the ProtonVPN application, selected the 'Fastest Free Server' option, and clicked Connect. Waited for confirmation of a successful connection.

- Verify IP Address Change: Checked IP address before connecting to VPN on WhatIsMyIPAddress.com. Checked again after connecting to VPN to confirm the location and IP had changed.

- Browse to Confirm Encryption: Opened websites and confirmed normal browsing activity while connected to VPN.

- Disconnect VPN and Compare: Disconnected from VPN and compared browsing speed and IP address with and without VPN.

## 5. Benefits of VPN

- Masks real IP address and location.

- Encrypts internet traffic to protect data from hackers and ISPs.

- Bypasses geographical restrictions for websites and services.

- Secures public Wi-Fi usage.

## 6. Limitations of VPN

- May reduce internet speed due to encryption and routing.

- Some websites block VPN traffic.

- Free VPNs may have limited server options and bandwidth.

- VPN does not guarantee complete anonymity.

## 7. Interview Questions and Answers

Q1: What is a VPN?

Ans: A VPN is a Virtual Private Network that encrypts your internet connection and routes it through a remote server.

Q2: How does a VPN protect privacy?

Ans: It hides your IP address and encrypts your internet traffic, preventing third parties from tracking your activities.

Q3: Difference between VPN and proxy?

Ans: A proxy only routes traffic through another server without encryption; a VPN encrypts traffic and hides your IP.

Q4: What is encryption in VPN?

Ans: Encryption is the process of converting data into a coded format that prevents unauthorized access.

Q5: Can VPN guarantee complete anonymity?

Ans: No. VPNs enhance privacy but do not provide 100% anonymity; other tracking methods can still be used.

Q6: What protocols do VPNs use?

Ans: Common protocols include OpenVPN, IKEv2/IPSec, and WireGuard.

Q7: What are some VPN limitations?

Ans: Slower speeds, server limitations, and possible blocking by certain websites.

Q8: How does a VPN affect network speed?

Ans: VPN encryption and routing may slow down speed, depending on server distance and load.

## 8. Conclusion

This task provided hands-on experience with VPN setup, usage, and verification. It reinforced the importance of VPNs in maintaining privacy and security online, as well as understanding their limitations.