Task 8 Report – VPN Setup and Analysis

# Objective

To understand and demonstrate the role of VPNs in enhancing privacy and enabling secure internet communication through hands-on testing with ProtonVPN and Windscribe VPN.

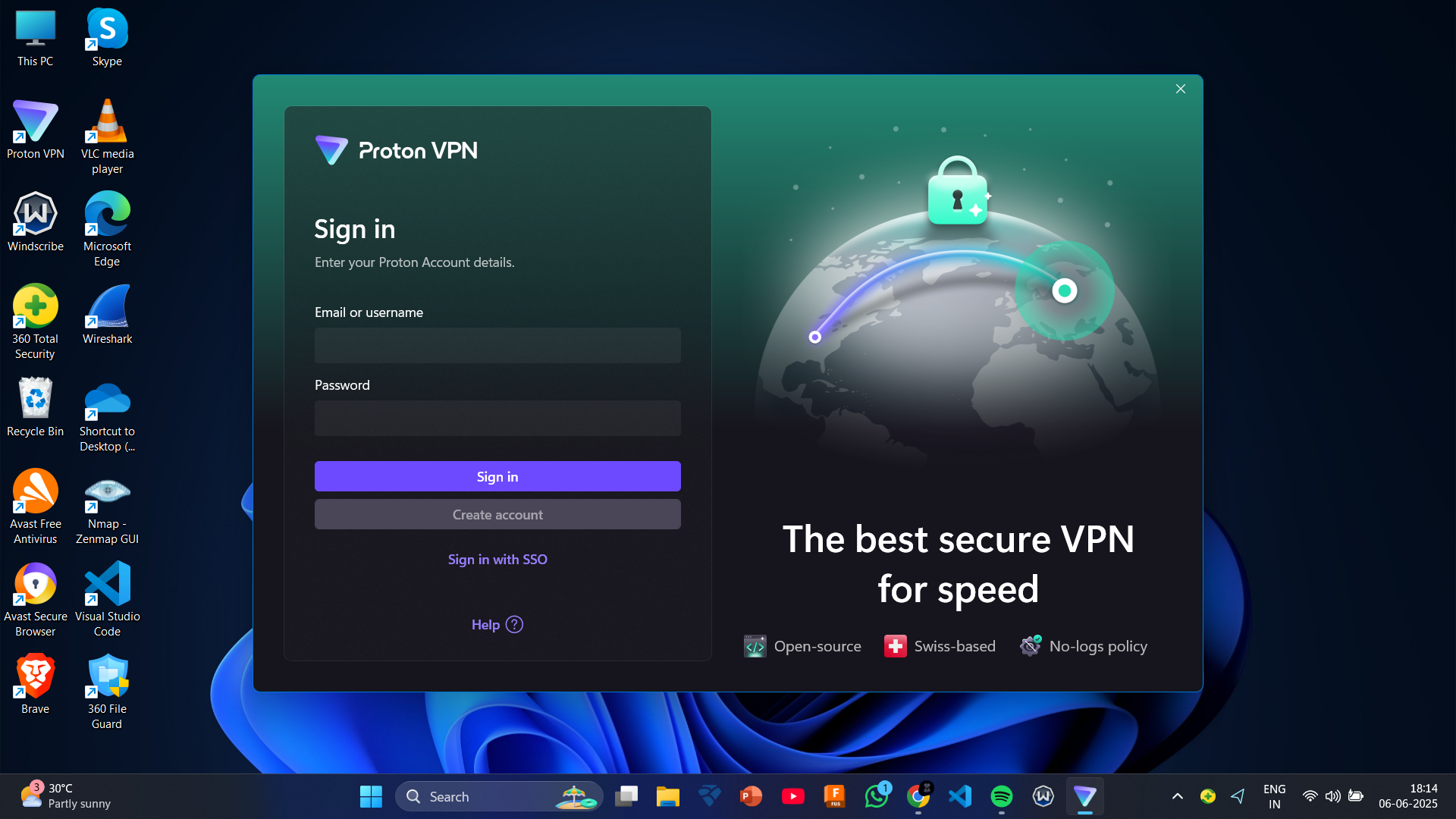
# Tools Used

1. ProtonVPN (Free Tier) – https://protonvpn.com  
2. Windscribe VPN (Free Tier) – https://windscribe.com  
3. https://whatismyipaddress.com (to verify IP changes)  
4. Speed testing and browser verification tools

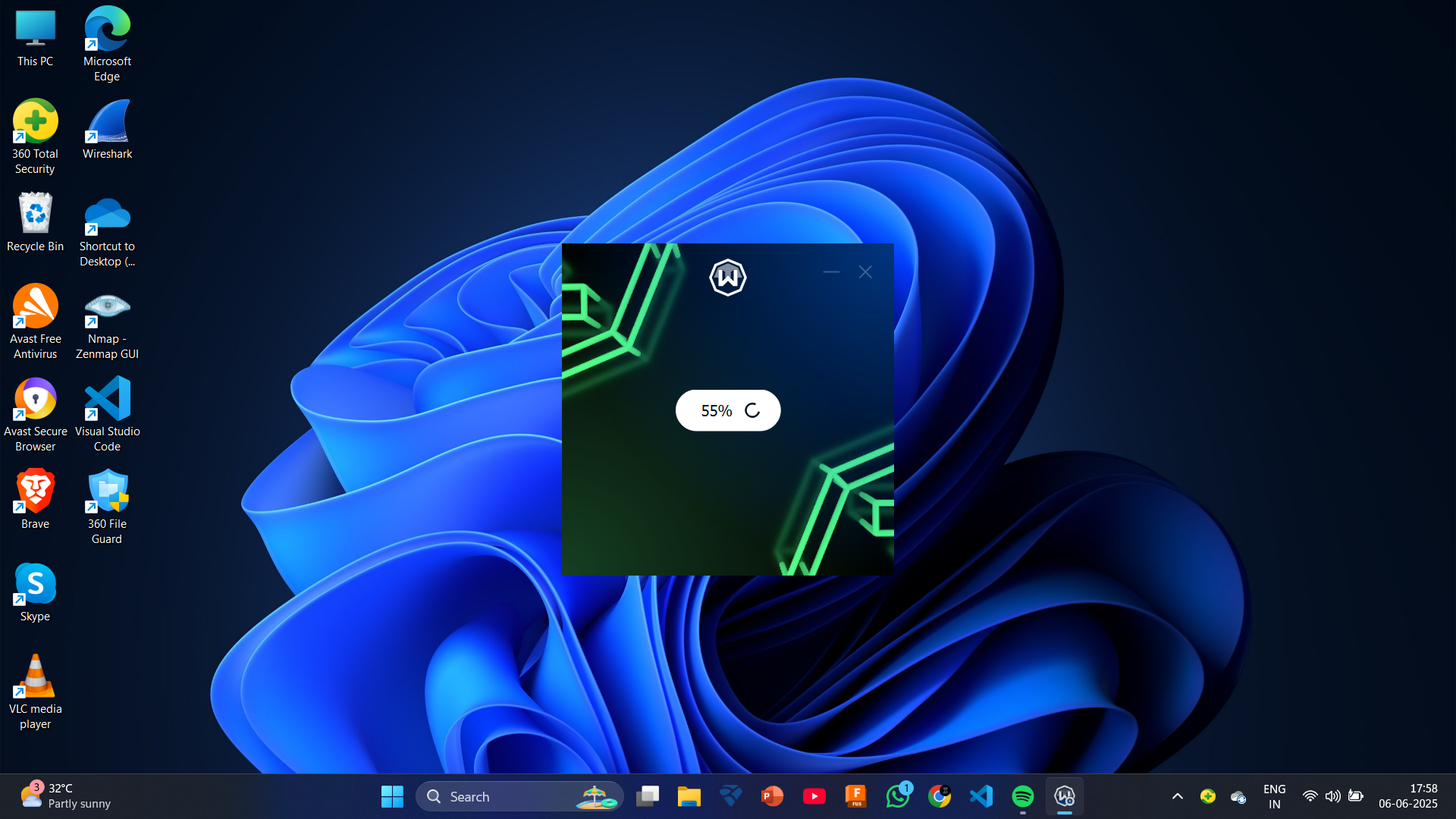
# Steps Performed

1. 1. Downloaded and installed ProtonVPN and Windscribe VPN clients from their official websites.
2. 2. Created free user accounts and signed in to both applications.
3. 3. Connected ProtonVPN to the default server. Verified VPN status and IP change.
4. 4. Connected Windscribe VPN to the 'Best Location' (Victoria). Observed the IP masking.
5. 5. Browsed secure websites and checked IP address changes to ensure encryption.
6. 6. Verified VPN status and performance by viewing app interfaces and public IPs.
7. 7. Captured screenshots to document successful VPN connections.

# Screenshots – VPN Connection Status







# Summary and Analysis

## Benefits Observed

- Both VPNs successfully masked the actual IP address, proving IP obfuscation.

- Traffic was encrypted, which helps protect against eavesdropping and surveillance.

- Free plans allowed basic testing and secure browsing.

- Useful in public Wi-Fi environments for securing communications.

## Limitations Noticed

- ProtonVPN required account creation and had limited free locations.

- Windscribe had a 2 GB/month data limit on the free tier.

- Slight decrease in internet speed when connected to remote servers.

- Free plans did not include premium features such as advanced streaming or multi-hop connections.