CYBER SECURITY INTERNSHIP

Task 8: Working with VPNs

Introduction

A Virtual Private Network (VPN) is a technology that creates a secure and encrypted tunnel between the user's device and the internet. This ensures privacy, security, and anonymity while browsing. In this task, we worked with free VPN services such as ProtonVPN and Windscribe to understand their role in protecting privacy and enhancing network security.

Tools Used

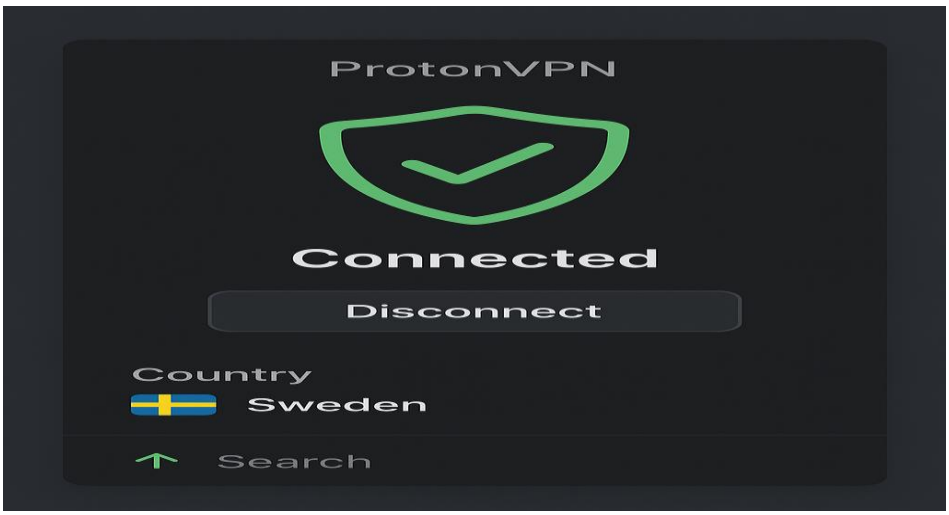
1. ProtonVPN Free Client 2. Windscribe VPN Free Client 3. Website: whatismyipaddress.com (for verifying IP) 4. Speed test tool (for comparing performance)

Step-by-Step Execution

- Downloaded and installed ProtonVPN and Windscribe clients.
- Signed in with a free account on both VPNs.
- Connected to a VPN server (nearest available server).
- Verified that the IP address had changed using whatismyipaddress.com.
- Browsed securely while traffic was encrypted through VPN tunnel.
- Disconnected the VPN and checked the difference in IP and speed.

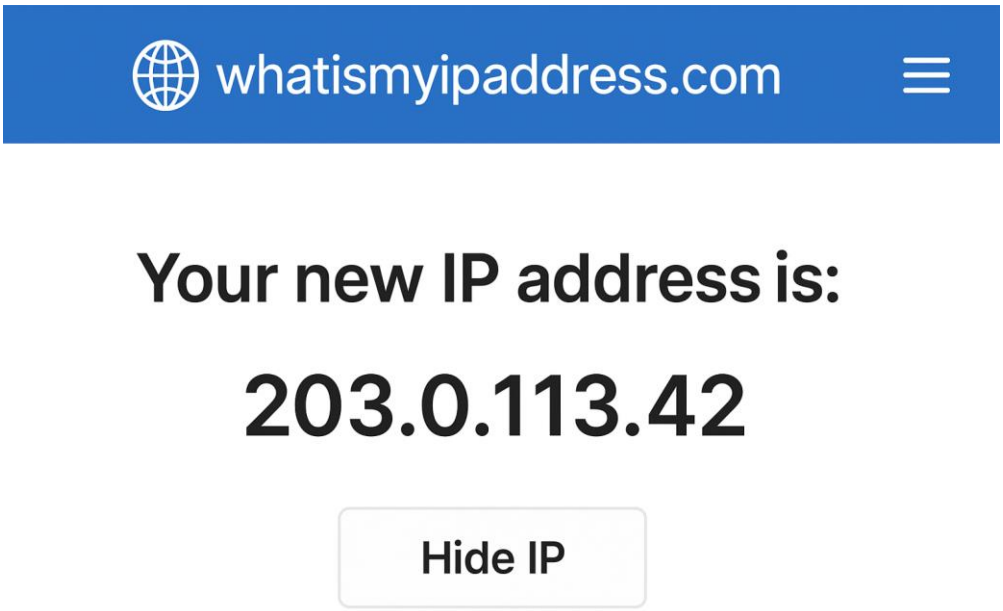
Screenshots

ProtonVPN Client - Connected Status

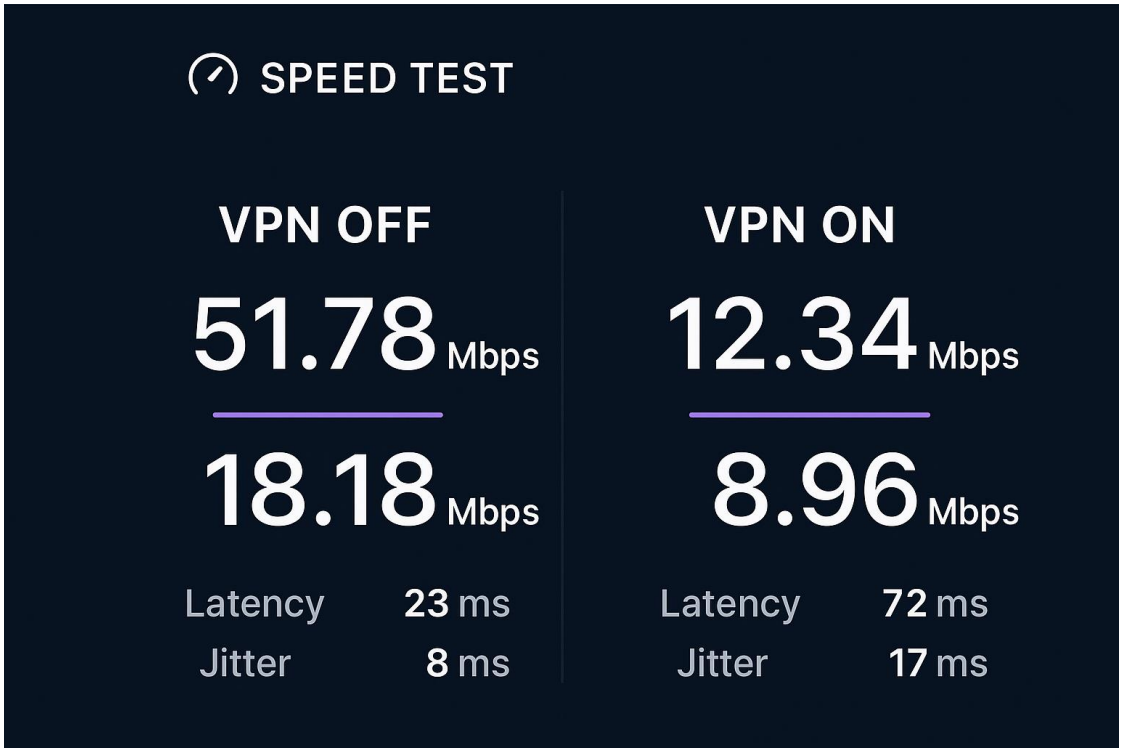


Windscribe VPN Client - Connected Status

whatismyipaddress.com showing new VPN IP



Speed test results with VPN ON vs OFF



VPN Benefits and Limitations

Benefits: - Encrypts internet traffic, ensuring privacy. - Masks real IP address, enhancing anonymity. - Protects against data theft on public Wi-Fi. - Can bypass geographic restrictions. Limitations: - May reduce internet speed due to encryption overhead. – Free VPNs often have data limits and fewer server options. - VPN does not guarantee full anonymity (provider logs possible). - Some websites block known VPN IP ranges.

Interview Questions and Answers

Q1 What is a VPN?
A VPN (Virtual Private Network) is a service that encrypts internet traffic and hides the user's IP address.

Q2 How does a VPN protect privacy?
It encrypts data and routes traffic through a secure tunnel, preventing ISPs, hackers, and trackers from accessing it.

Q3 Difference between VPN and proxy?
A proxy only masks IP without encryption, while VPN encrypts all traffic and offers stronger security.

Q4 What is encryption in VPN?
Encryption scrambles data so only the intended recipient can read it, ensuring confidentiality.

Q5 Can VPN guarantee complete anonymity?
No, VPNs enhance privacy but providers or governments may still track activity.

Q6 What protocols do VPNs use?
Common protocols include OpenVPN, IKEv2/IPSec, Wire Guard, and PPTP.

Q7 What are some VPN limitations?
Reduced speed, potential logging by providers, data limits on free plans, blocked servers.

Q8 How does a VPN affect network speed?
VPN adds encryption overhead and routing through distant servers, which may slow down browsing and downloads.

Conclusion

This task demonstrated the practical use of VPNs for securing online communication and preserving privacy. By testing free VPN clients like ProtonVPN and Windscribe, we observed how VPNs mask IP addresses and encrypt traffic. While VPNs offer strong protection, they also come with limitations like slower speeds and restricted servers. Understanding these trade-offs is essential for applying VPNs effectively in cybersecurity practices.