TASK 8 : WORKING WITH VPNs

Objective: Understand the role of VPNs in protecting privacy and secure communication.

Tools: Free VPN client (ProtonVPN free tier, Windscribe free)

.

Internship: Elevate Labs,

Prepared by: P. SUSMITHA,

Date: 31/10/2025.

Virtual Private Network

A VPN (Virtual Private Network) is a security tool that creates a secure, encrypted connection between your device and the internet. It acts as a private tunnel through which your data travels safely, protecting it from hackers, trackers, and other online threats.

When you connect to a VPN, your internet traffic is routed through a remote VPN server instead of your Internet Service Provider (ISP). This process hides your real IP address and replaces it with the server's IP address, making your online identity and location invisible to outsiders.

Key Functions of a VPN:

1. Encrypts Data: Converts your data into unreadable code, ensuring no one (even your ISP or hackers) can intercept it.

2. Hides IP Address: Replaces your real IP address with the VPN server's IP, making your browsing anonymous.

3. Secure Remote Access: Allows users to securely access private networks (like office systems) from anywhere.

4. Protects Public Wi-Fi Usage:
VPNs safeguard your data from cyberattacks while using public or unsecured Wi-Fi networks.

5. Bypasses Geo-Restrictions: Lets you access content or websites restricted to certain regions (like streaming services or research databases).

Working of VPN:
- You connect to a VPN server through an application.
- The VPN encrypts your internet traffic.
- The encrypted data passes through a secure tunnel to the server.
- The server then communicates with websites or services on your behalf.
- The website only sees the VPN server's IP, not your real one.

Common VPN Protocols:

OpenVPN:- Most secure and commonly used.
IKEv2/IPsec:- Fast and stable, good for mobile devices.
WireGuard:- Modern and lightweight with strong encryption.
L2TP/IPsec:- Offers strong encryption but slower.

Benefits of Using a VPN:

Ensures online privacy and anonymity.
Protects data from hackers, trackers, and advertisers.
Secures connection over public Wi-Fi.
Prevents ISP monitoring and bandwidth throttling.
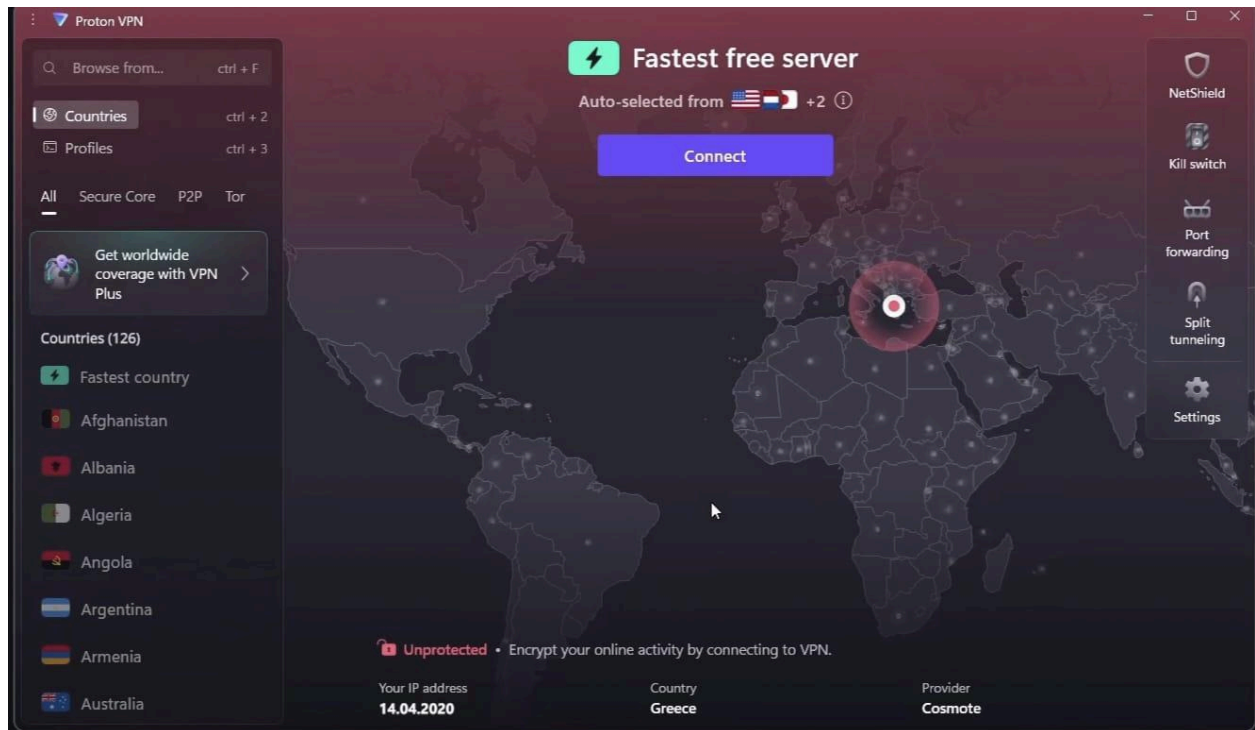Enables remote work securely.

Limitations of a VPN:

May cause a slight drop in internet speed due to encryption.
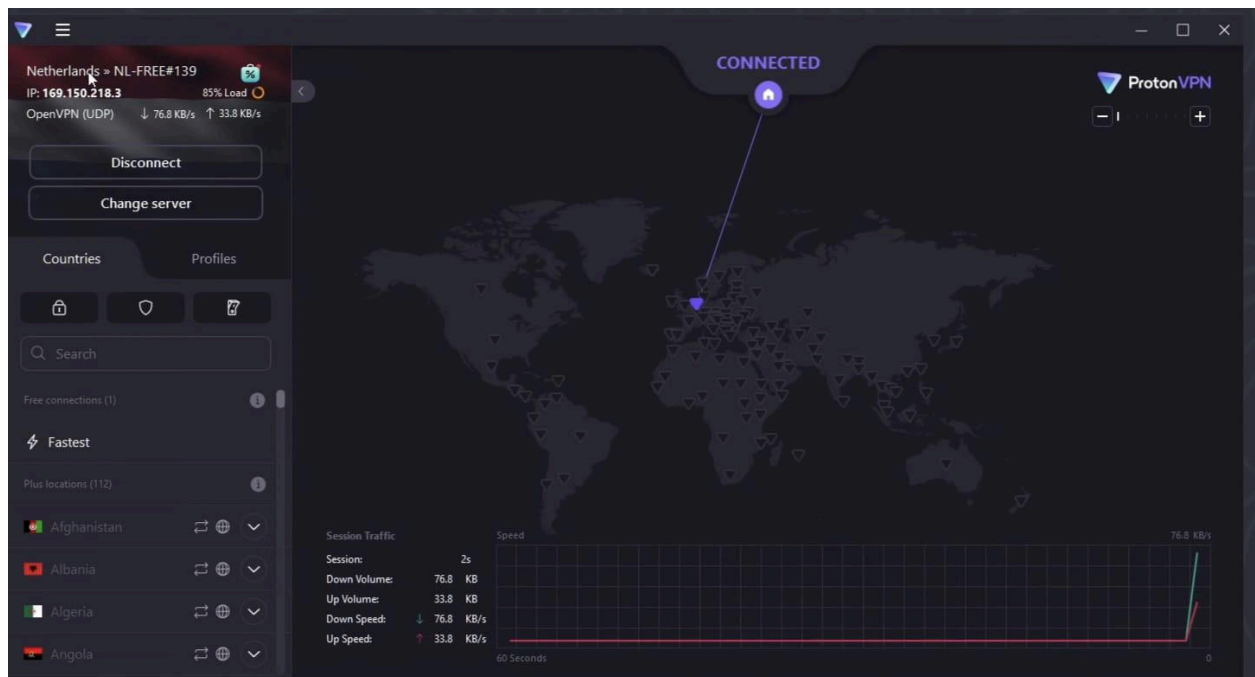Some free VPNs have data limits or weaker security.
VPNs cannot protect against malware or phishing directly.
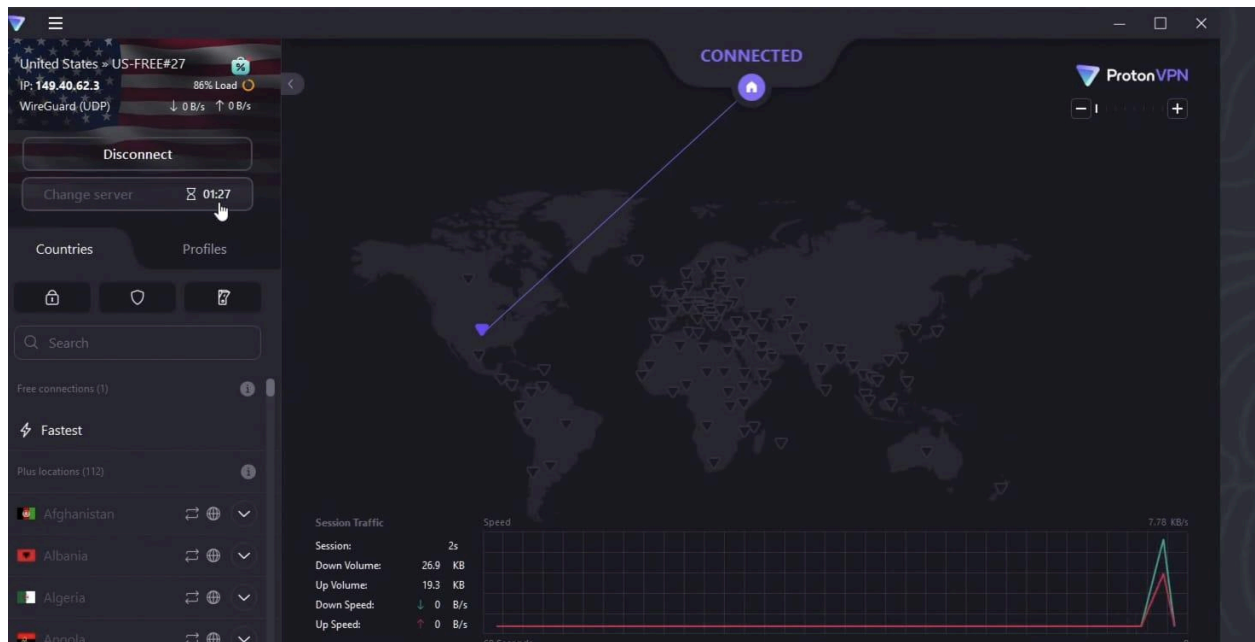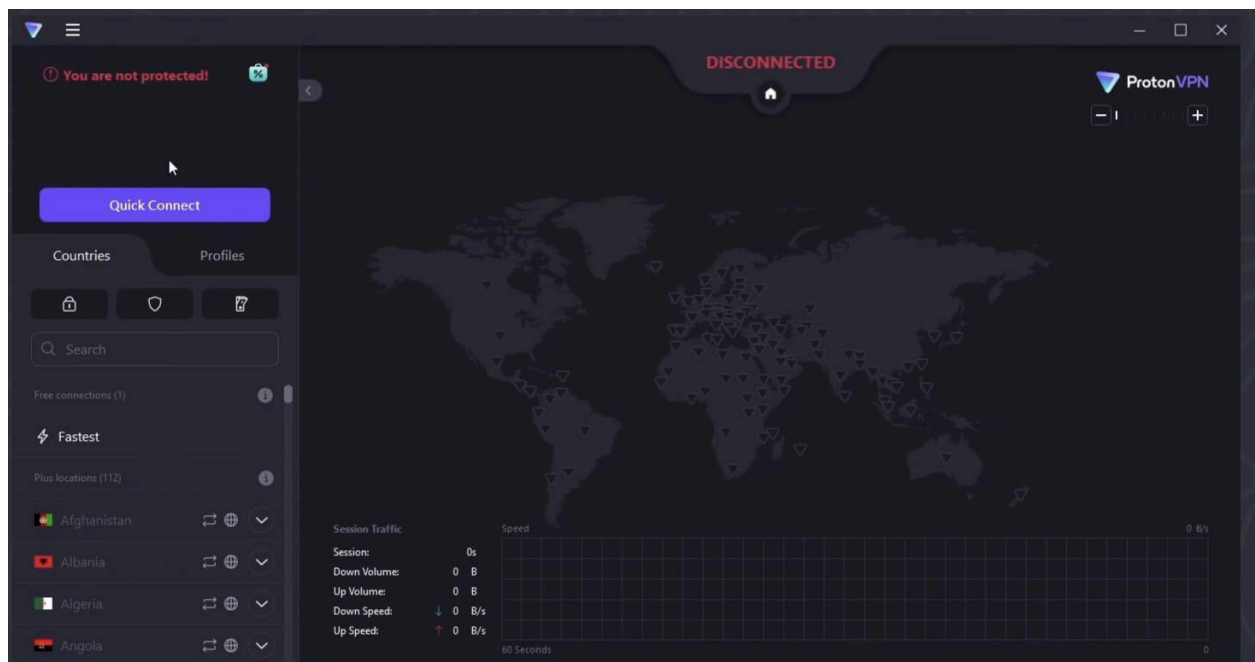Not all VPNs guarantee complete anonymity.

Screenshots:

figure(1): ProtonVPN dashboard on Windows

figure(2): ProtonVPN successfully connected to a server in Netherlands.

figure(3): ProtonVPN connected to a United States Server.

figure(4): VPN in a disconnected state.