

VPN Privacy and Secure Communication

Name: Pulak Jindal

Task No.: 8

Date: 1st November, 2025

Objective

To understand how VPNs enhance privacy, secure online communication, and hide IP addresses by encrypting traffic through secure tunnels.

Tools Used

- **VPN Client:** ProtonVPN
- **Website for IP check:** whatismyipaddress.com
- **Browser:** Edge

Procedure

1. Created an account on Proton VPN
2. Installed and launched the VPN client.
3. Connected to the VPN server located in Netherland.
4. Verified IP address change using whatismyipaddress.com.
5. Checked browsing encryption (lock icon, HTTPS).
6. Disconnected VPN and noted change in speed and IP address.

Note: The VPN was initially tested on college Wi-Fi, but the connection failed due to VPN traffic restrictions. The test was later performed on a mobile hotspot network.

Results

Condition	IP Address	Location	Speed (Subjective)
Without VPN	192.138.168.6	India	Fast
With VPN	10.17.34.67	Netherlands	Slightly slower

VPN Encryption and Privacy Features

- Uses **AES-256 encryption** (military-grade).
- Tunnels traffic through **OpenVPN / WireGuard protocols**.
- **No-log policy:** prevents recording user activity.
- **Kill Switch:** stops internet if VPN drops.
- **DNS leak protection:** prevents exposure of real IP.

Benefits

- Hides real IP and location.
- Protects data on public Wi-Fi.
- Prevents tracking and profiling.
- Accesses geo-blocked content securely.

Limitations

- Can reduce browsing speed.
- Some websites block VPN traffic.
- Free versions may have limited servers or bandwidth.
- Cannot protect against malware if user downloads infected files.

Conclusion

The VPN successfully changed the IP address and encrypted all traffic, demonstrating how VPNs safeguard privacy and ensure secure communication. However, VPN restrictions on institutional networks can limit usage.