Cyber Security Internship - Task 8 Report: VPN Analysis

1. Introduction and Objective

The primary objective of this task was to gain practical experience with a Virtual Private Network (VPN) client to understand its role in enhancing user privacy and securing online communication channels.

Detail	Value
Task Focus	Understanding VPNs, Encryption, and Network Security.
Tool Used	ProtonVPN Free Tier client, whatismyipaddress.com.
Deliverables	Report on VPN setup, connection verification, and summary of benefits/limitations.

2. Deliverable 1: Report Describing VPN Setup Steps

The **ProtonVPN Free Tier** client was selected and utilized for this hands-on task.

VPN Setup and Connection Steps

1. **Client Selection and Installation:** A reputable free VPN client, ProtonVPN, was chosen, and the application was successfully downloaded and installed on the local system.
2. **Verification Preparation:** The original public IP address was documented using \texttt{whatismyipaddress.com} to establish a baseline.
3. **Connection Establishment:** The VPN client was launched, and a secure connection was established to an available VPN server located in the Netherlands.
4. **Verification Confirmation:** The public IP address was checked again post-connection to confirm the change.

3. Deliverable 1: Connection Status Verification

The comparison of the network status before and after activating the VPN confirms that the public identity has been successfully masked, routing traffic through the secure VPN server.
Note: The visual evidence (screenshots) confirming this IP address change has been organized and included in the separate \texttt{screenshots/} directory within the GitHub repository.

IP Address Comparison Table (Evidence of VPN Functionality)

Field	Pre-VPN Status (Original)	Post-VPN Status (VPN Tunnel)
Public IPv4	103.230.149.236	89.105.214.103
Location	Mumbai, India	Doetinchem, Netherlands
ISP/Service	Google LLC / Data Center	Novoserve B.V. / VPN Server

The successful change in IP address, location, and ISP confirms that all internet traffic is being correctly routed through the encrypted VPN tunnel.

4. Deliverable 2: Summary of VPN Benefits and Limitations

Key Benefits of VPNs

- **Data Encryption:** A VPN uses robust encryption protocols (e.g., AES-256) to create a secure tunnel for all traffic, crucial for maintaining **confidentiality** and preventing data interception over unsecured networks.
- **Privacy and Identity Masking:** By replacing the user's real public IP address with the VPN server's IP, the VPN prevents tracking by ISPs, advertisers, and trackers, protecting the user's digital footprint.
- **Enhanced Security:** The encrypted connection is vital for maintaining security when connected to public or untrusted Wi-Fi hotspots.

Inherent Limitations of VPNs

- **Reduced Network Speed:** The extra processes of encrypting/decrypting data and routing traffic through a remote server introduce latency, often resulting in slower connection speeds.
- **Dependence on Provider Trust:** A user's privacy depends entirely on the VPN provider's commitment to a **No-Logging Policy**. If logs are kept, the provider becomes a central point of potential surveillance.
- **Not a Complete Solution:** A VPN secures the connection but does not protect against all threats (e.g., phishing, malware, or willingly submitting personal information). It must be part of a broader security strategy.

5. Conclusion

The execution of Task 8 confirmed the practical utility of a VPN in securing an internet connection and masking the user's true identity. This hands-on verification, combined with the research summary, highlights the VPN's critical role in modern network security and digital privacy.