Task 8 — Set up and Use a VPN

Author: Yuvraj Yadav
Date: 31-10-2025
Platform Used: macOS
VPN Used: ProtonVPN (Free Tier)

1 Objective

The objective of this task was to install and configure a **VPN (Virtual Private Network)** on macOS to experience secure, encrypted internet communication.
The task aimed to verify IP masking, understand VPN encryption concepts, and observe the effects on connection speed and privacy.

2 Tools and Environment Setup

Operating System: macOS
VPN Tool: ProtonVPN (Free Tier)
Browser Used: Google Chrome

Installation Steps:

1. Signed up for a free account on https://protonvpn.com.
2. Downloaded and installed the **ProtonVPN macOS client**.
3. Logged in using free account credentials.

3 Steps Performed

Step 1 — Launch and Login

- Opened ProtonVPN and logged in.
- Dashboard displayed multiple VPN servers (Free and Premium).

Step 2 — Connect to VPN Server

- Selected **“Netherlands (Free)”** server.
- Clicked **Connect**.
- Connection established successfully with AES-256 encrypted tunnel.

Screenshot:
`01_vpn_connected.png` — ProtonVPN dashboard showing active connection.

Step 3 — Verify IP Address

Before connecting:

- Checked IP via [whatismyipaddress.com] → `49.xxx.xxx.xx` (India)

After connecting:

- New IP: `185.xxx.xxx.xx` (Netherlands)

IP changed successfully → confirming encrypted tunneling.

Step 4 — Test Encryption & Speed

- Accessed multiple websites — all loaded correctly.
- Verified HTTPS padlock remained active.
- Measured browsing speed — slightly reduced (~10–15%) due to encryption overhead.

Step 5 — Disconnect and Compare

- Disconnected VPN connection.
- Rechecked IP — reverted back to original (India-based).
- Browsing speed improved slightly.

4 Analysis

Parameter	Without VPN	With VPN
IP Location	India	Netherlands
Encryption	None	AES-256
Latency	Low	Moderate
Privacy	Standard	Enhanced
ISP Visibility	Full	Hidden

5 Security Insights

- **VPN (Virtual Private Network)** creates an **encrypted tunnel** between the client and VPN server, ensuring that no third party (like ISPs) can view browsing activity.
- Encrypts traffic using **AES-256-**bit encryption with **OpenVPN / WireGuard protocols**.
- Masks real IP address → improving **anonymity and privacy**.
- **Limitations:**
    - Reduced browsing speed due to encryption.
    - Trust depends on the VPN provider’s logging policy.
    - Not a substitute for good browser hygiene.

6 Key Learnings

- Learned to configure and use VPN safely on macOS.
- Observed how **IP masking** protects against tracking.

- Understood the basics of **VPN tunneling protocols (OpenVPN, IKEv2, WireGuard)**.
- Verified encryption and connection stability through IP change test.

7 Outcome

Successfully set up and used a **VPN** for secure browsing and IP masking.
Understood the working of VPN encryption, tunneling, and privacy benefits.
Captured screenshots for connection verification and IP testing.

Skills Gained:

- VPN installation and configuration
- IP masking verification
- Encryption and tunneling understanding
- Privacy and data protection awareness

8 Attachments (for GitHub Repo)

1. **Screenshots Folder:**
    - `01_vpn_connected.png`
    - `02_ip_before.png`
    - `03_ip_after.png`
    - `04_disconnect.png`
2. **report.md** — this detailed documentation
3. **README.md** — summary of setup and analysis