**Task – 8**

**Working with VPNs**

**Step 1. VPN Selection**

I chose ProtonVPN Free Tier due to its strong privacy policies, Swiss-based jurisdiction (strong privacy laws), and no-logs policy.

**Step 2. Setup steps**

a) Sign up

b) Download and Install

c)Login and connect

**Step 3. Connection Verification**

* Before VPN: IP shown as my local ISP location.
* After VPN: IP changed to VPN server location (e.g., Netherlands).

**Screenshot of connection status and IP address after VPN connection**

**4. Encrypted Browsing Test**

* Visited a website (e.g., <https://example.com>).
* Confirmed HTTPS traffic encryption (lock icon in browser).
* Verified that traffic was routed through VPN by checking IP in browser dev tools or IP sites.

**5. VPN Disconnection & Comparison**

* Disconnected from VPN.
* Browsing speed increased slightly (~10-15% faster).
* IP reverted back to ISP location.

**6. VPN Encryption and Privacy Features (Research)**

* ProtonVPN uses **AES-256 encryption** with **OpenVPN** and **WireGuard** protocols.
* Supports **Perfect Forward Secrecy**.
* Operates under a strict **No-Logs policy**.
* Allows **DNS leak protection** and **kill switch** (in paid tier or manual setup).

**7. VPN Benefits and Limitations**

**Benefits**

* Hides IP address and location.
* Encrypts data traffic, especially useful on public Wi-Fi.
* Access to geo-blocked content.
* Prevents ISP tracking.

**Limitations**

* Free tiers have limited server choices and slower speeds.
* Doesn’t make you completely anonymous.
* Some websites may block VPN IPs.
* Trust still required in VPN provider (logs, policies).



