**Task 8: Using a VPN and Managing Browser Extensions**

**Objective**

* To explore how a VPN improves online privacy and to identify any browser extensions that may pose a security risk.

**System Information**

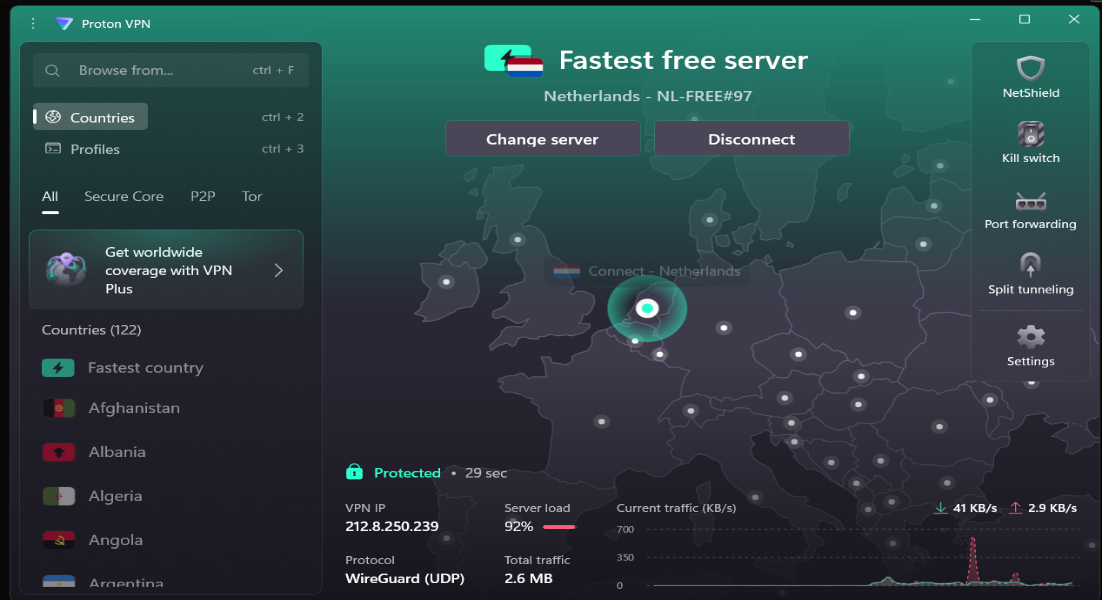
* **Operating System**: Windows 64-bit
* **VPN Tool Used**: ProtonVPN (Free version)

**Step 1: Installing ProtonVPN**

* To start, a secure VPN was needed. ProtonVPN was chosen because it is trusted, free to use, and provides secure internet access without logging user data.
* **Steps Taken:**
* Visited the official website: [protonvpn.com](https://protonvpn.com)
* Downloaded the VPN software for Windows
* Installed the application and created a free user account
* Launched the app and logged in

**Step 2: Connecting to the VPN**

* Once ProtonVPN was open:
* Selected a free server from the list
* Clicked "Connect"
* The app showed a new IP address and confirmed the connection was secure
* This ensured that internet traffic was encrypted and protected from outside tracking



**3. IP Address Verification**

To check whether the VPN masked the real IP:

* Visited <https://whatismyipaddress.com>
* Observed a new IP address and virtual location (e.g., Chicago, USA)
* This IP address was different from the original one shown before connecting

This confirmed that ProtonVPN was successfully hiding the real IP address and routing internet traffic through a VPN server.

**A screenshot of a computer

AI-generated content may be incorrect.**

**4. Encrypted Connection Confirmation**

To ensure the website connection was secure, I accessed <https://duckduckgo.com>. The following indicators confirmed that the connection was encrypted:

* The URL began with https://, indicating a secure protocol.
* A padlock icon was visible in the address bar.
* Clicking the padlock showed the message: “Connection is secure” in Google Chrome.

These signs confirmed that SSL/TLS encryption was in place for safe data transmission. Additionally, the active VPN tunnel added another layer of security, encrypting all outgoing and incoming internet traffic.

**5. VPN Disconnect and IP/Speed Check**

After disconnecting from ProtonVPN, I revisited <https://whatismyipaddress.com> to verify the changes. The original IP address and actual geographic location were now visible, confirming that the VPN was no longer active.

**Browsing Speed Observation:**

* **Without VPN**: Webpages loaded slightly faster due to the direct connection without encryption overhead.
* **With VPN**: There was a minor reduction in speed, which is expected because data is encrypted and routed through remote servers.

Overall, the slight decrease in speed while using the VPN was acceptable, given the increased privacy and security benefits.

A screenshot of a computer

AI-generated content may be incorrect.

**6. How ProtonVPN Protects Your Privacy**

* **Strong Encryption**: ProtonVPN uses top-grade encryption (AES-256) to keep your internet activity safe from hackers, especially on public Wi-Fi.
* **Secure Connection Protocols**: It uses trusted protocols like **OpenVPN** and **WireGuard** to build a safe path for your data to travel through.
* **No Browsing History Saved**: ProtonVPN follows a strict **no-log policy**, meaning it does **not store** what websites you visit or what you do online.
* **IP Address Protection**: Your real IP address is hidden, so websites can’t track your real location.
* **DNS Leak Protection**: Even your DNS requests (like visiting a website) are hidden from your internet provider.
* **Kill Switch Feature**: If the VPN disconnects suddenly, it **immediately stops your internet**, so your real identity isn’t exposed.
* **New Encryption Every Time**: Each time you connect, ProtonVPN creates a **new encryption key**, making it extra hard for hackers to crack past sessions.

**7. VPN – Benefits and Limitations**

**Main Benefits of Using a VPN:**

* **Stay Anonymous Online**: Hides your real location and IP address.
* **Secure Public Wi-Fi**: Protects your data when using free Wi-Fi in cafes, airports, etc.
* **Access Blocked Sites**: Helps open websites or apps blocked in your region or country.
* **Avoid Online Tracking**: Stops ISPs and trackers from spying on your activity.
* **Safe Communication**: Keeps chats, passwords, and emails protected from theft.
* **Limitations of Free VPN Services (like ProtonVPN Free):**
* **Limited Server Options**: You can only connect to a few countries.
* **Slower Speed**: During busy hours, free servers may become slow.
* **No P2P or Streaming Support**: Some features like torrenting or video streaming are locked behind paid plans.
* **Risk if Kill Switch is Off**: If the VPN turns off and Kill Switch is not enabled, your real location may get exposed.

**8. Final Thoughts**

ProtonVPN offers excellent privacy tools, even in its free version. It protects users from online spying, secures data on public Wi-Fi, and allows access to blocked websites. While the free plan has limits like slower speed and fewer servers, it is still one of the most trusted and privacy-focused VPNs available. Ideal for students, travelers, and anyone who values safe and private internet browsing.