**Week 3: Encryption, VPNs & Security Protocols**

**Objective:** Study encryption standards and secure communication protocols.

**Task#02: Install OpenVPN or use a VPN client — configure and test your first VPN connection.**

**Solution:**

**Configuring and Testing Your First VPN Connection**

This guide outlines the general steps for installing and configuring a VPN client, focusing on OpenVPN as a common example.

* **OpenVPN Client:** This is an open-source VPN solution that requires you to obtain configuration files (usually .ovpn files) from a VPN provider or a self-hosted VPN server. It offers strong encryption and flexibility.

**2. Installation of the VPN Client**

**For OpenVPN Client (e.g., OpenVPN GUI for Windows)**

1. **Download:** Visit the official OpenVPN website or a trusted source (e.g., community versions like OpenVPN GUI for Windows).
2. **Select OS:** Download the appropriate installer for your operating system.
3. **Run Installer:** Execute the downloaded installer. Accept the license agreement and follow the default installation prompts.
4. **Launch:** After installation, the OpenVPN client will typically run in the background or be accessible from your system tray/menu bar.

**3. Configure Your VPN Connection**

**For OpenVPN Client:**

1. **Obtain Configuration File(s):** Get the. ovpn configuration file(s) from your VPN provider or server administrator. These files contain the necessary server details, certificates, and keys.
2. **Import Configuration:**
   * **Windows (OpenVPN GUI):** Copy the .ovpn file(s) to the config subfolder within your OpenVPN installation directory (e.g., C:\Program Files\OpenVPN\config). Right-click the OpenVPN GUI icon in the system tray and select "Import file..." or the configuration file name.
3. **Enter Credentials (if required):** If the .ovpn file requires a username and password (you can fetch it from the vendors website, from where you downloaded the .ovpn files) the client will prompt you for these when you attempt to connect.

**4. Test Your VPN Connection**

After initiating the connection, it's crucial to verify that your VPN is working correctly and your IP address has changed.

1. **Disconnect from VPN:** Temporarily disconnect your VPN.
2. **Check Public IP (Without VPN):** Open your web browser and go to a "What is my IP" website (e.g., whatismyip.com, iplocation.net). Note down your public IP address and location. This is your actual, unmasked IP.
3. **Connect to VPN:** Reconnect your VPN client. Wait until it indicates a successful connection.
4. **Check Public IP (With VPN):** Refresh the "What is my IP" website. Your displayed IP address and location should now be different, corresponding to the VPN server's location.

**Screenshots:**



