Task - 8

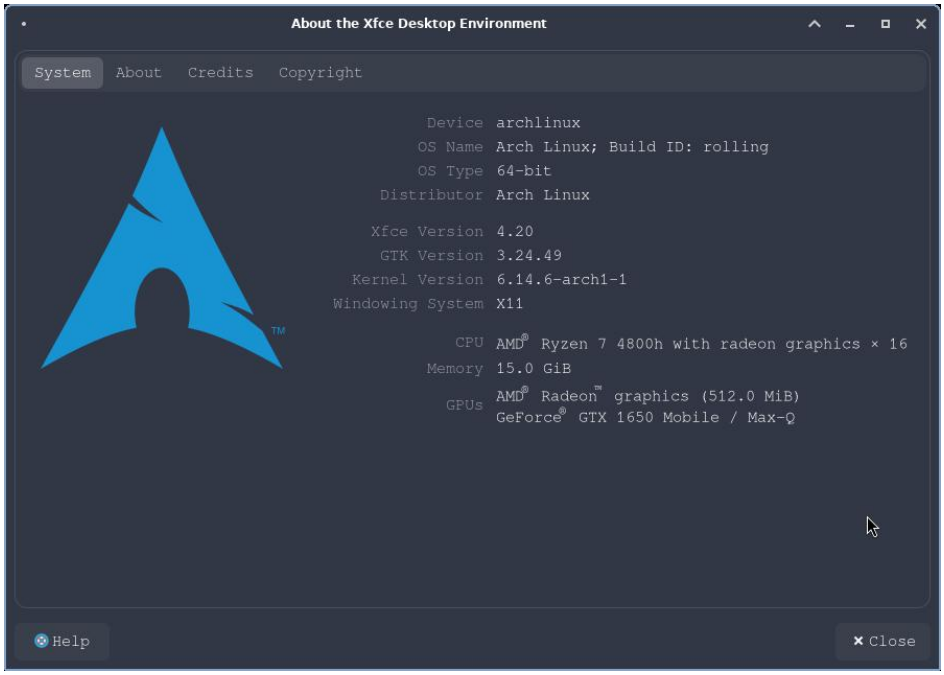
Virtual Private Network

Objective: Understand the role of VPNs in protecting privacy and secure communication

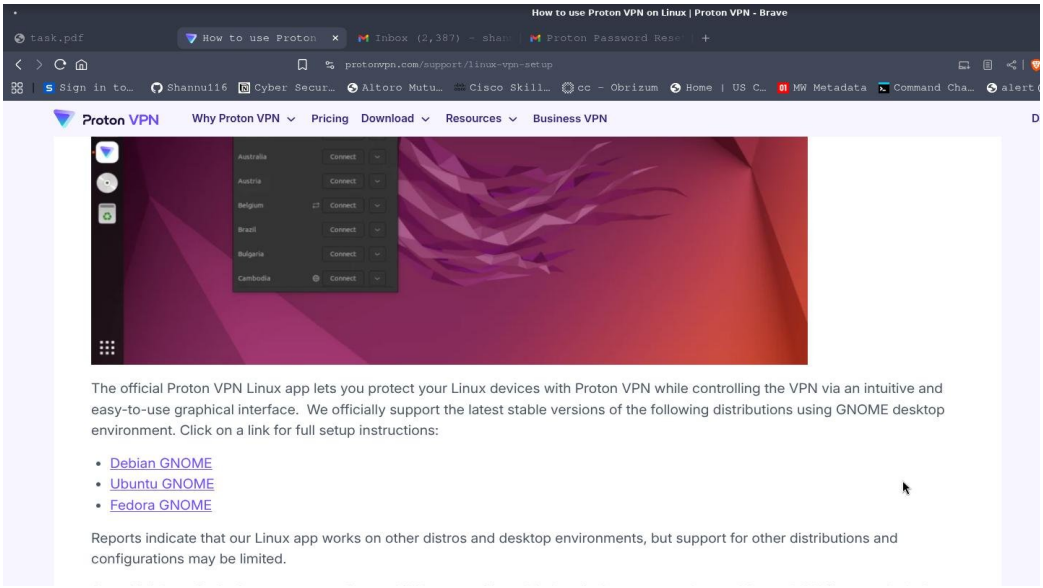
Tool: Free VPN client (ProtonVPN free tier, Windscribe free)

Process:

In this task we used the ProtonVPN with free tier, on kali linux because due to my host os is archlinux, i couldn't find the original protonVPN package for the arch distribution, and third party application may be not to be always trusted, So i proceeded with using it with in kali linux.



available options By the proton to use the application are Ubuntu,Debian , Fedora



Now we install the ProtonVPN in Kali according to the Instructions by the Instructed in the web page

When you click on the Debian GNOME, you will redirected in to next page, there you will have the instructions for the installation

To install the app, open a terminal window and:

1. Download the package that contains the repository configuration and keys required to install the Proton VPN app. Enter:

```
wget https://repo.protonvpn.com/debian/dists/stable/main/binary-all/protonvpn-stable-release_1.0.8_all.deb
```

2. Install the Proton VPN repository containing the app. Enter:

```
sudo dpkg -i ./protonvpn-stable-release_1.0.8_all.deb && sudo apt update
```

Please **don't try to check the GPG signature of this release package** (dpkg-sig –verify). Our internal release process is split into several parts; the release package is signed with a GPG key, and the repo is signed with another GPG key. So the keys don't match.

If you want to check the repo package's integrity, you can verify its checksum with the following command:

```
echo "0b14e71586b22e498eb20926c48c7b434b751149b1f2af9902ef1cfe6b03e180 protonvpn-stable-release_1.0.8_all.deb" |
sha256sum --check -
```

3. Install the app. Run:

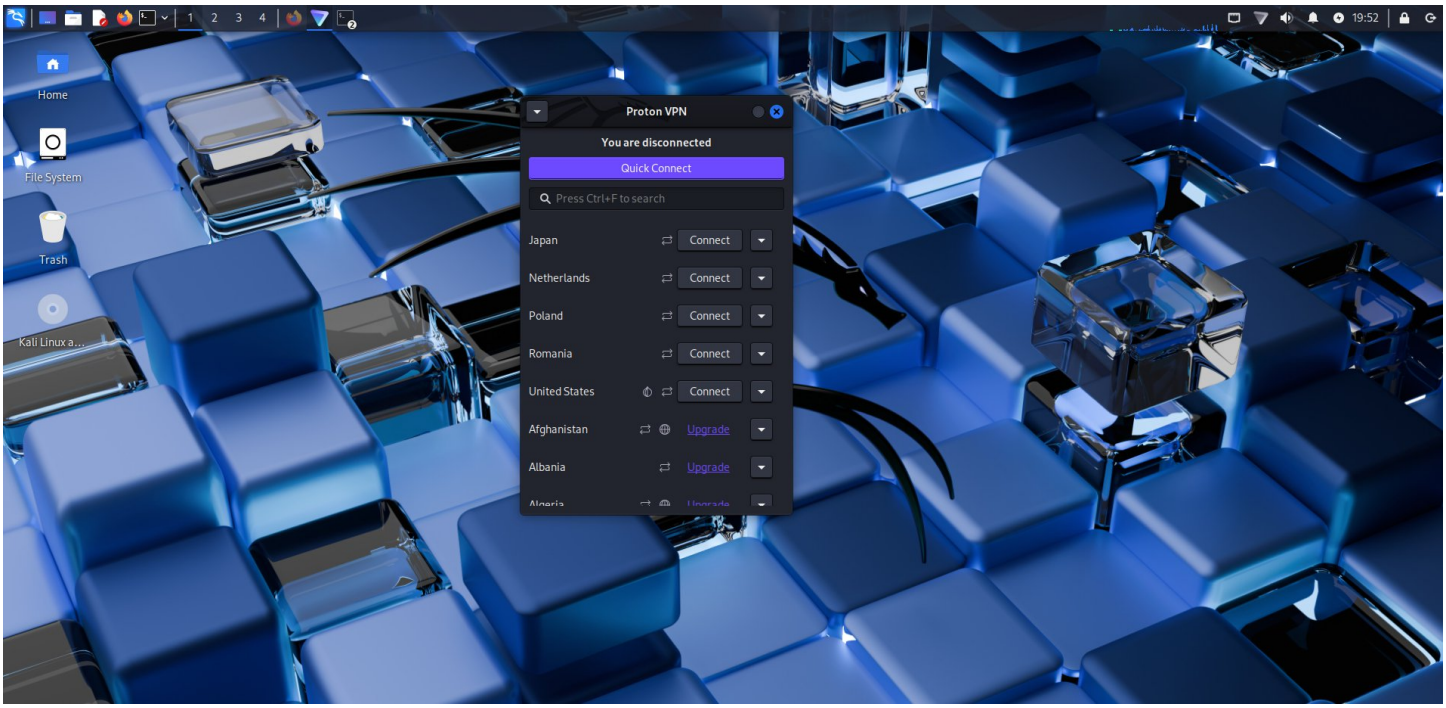
```
sudo apt install proton-vpn-gnome-desktop
```

Linux system tray icon **(optional)**

With 1st and 2nd command , you can install the protonVPN, next for the desktop ICON, use the last command

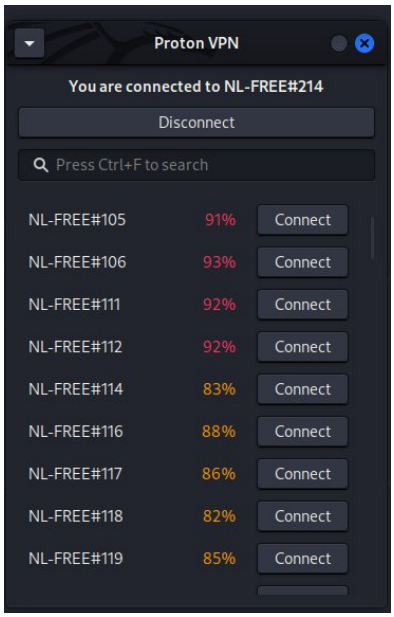
Command: sudo apt install proton-vpn-gnome-desktop

Next create an account , if you are using it in mobile you can use it as guest with no login, but here we must sign in , after sign in it opens like this tab

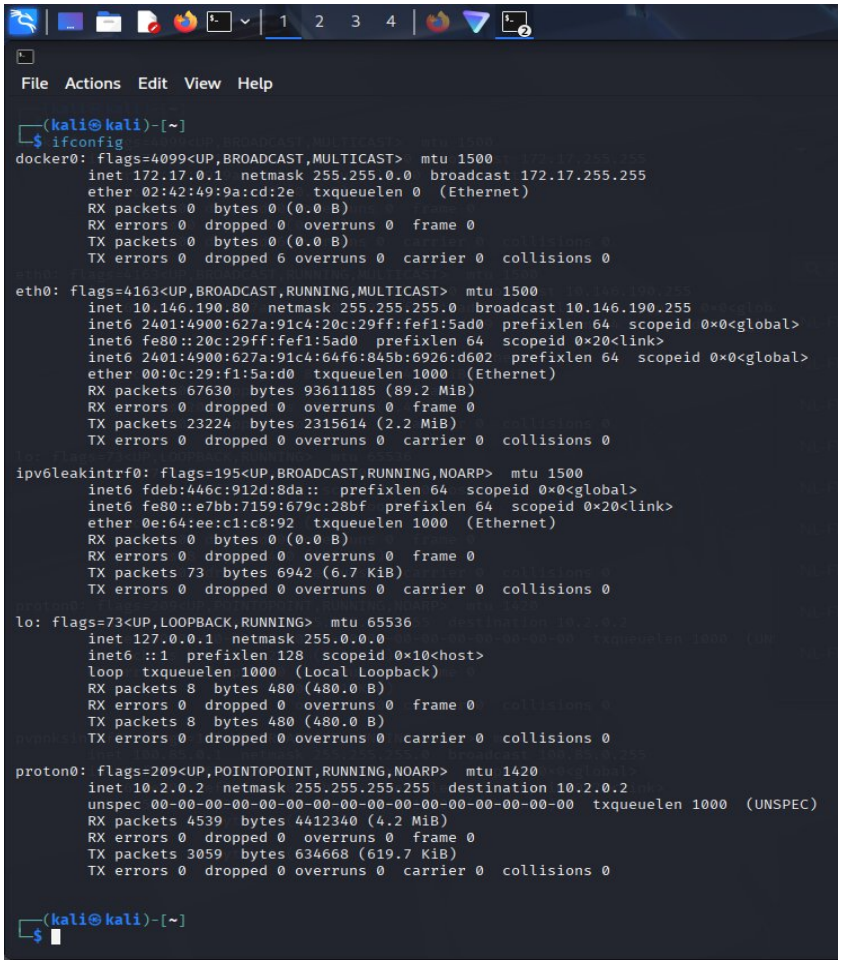


As you see, in free tier it offers only 5 , different servers to connect next click on the quick connect then it connects with the fastest server available in your tier.

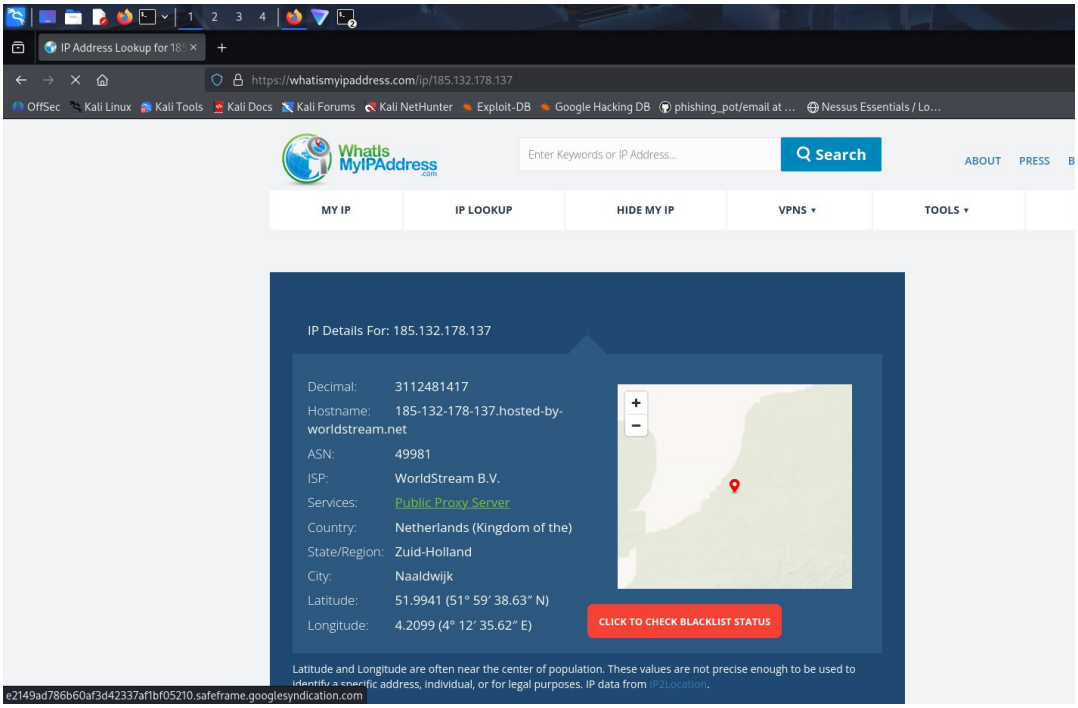
For me it connected to Netherlands



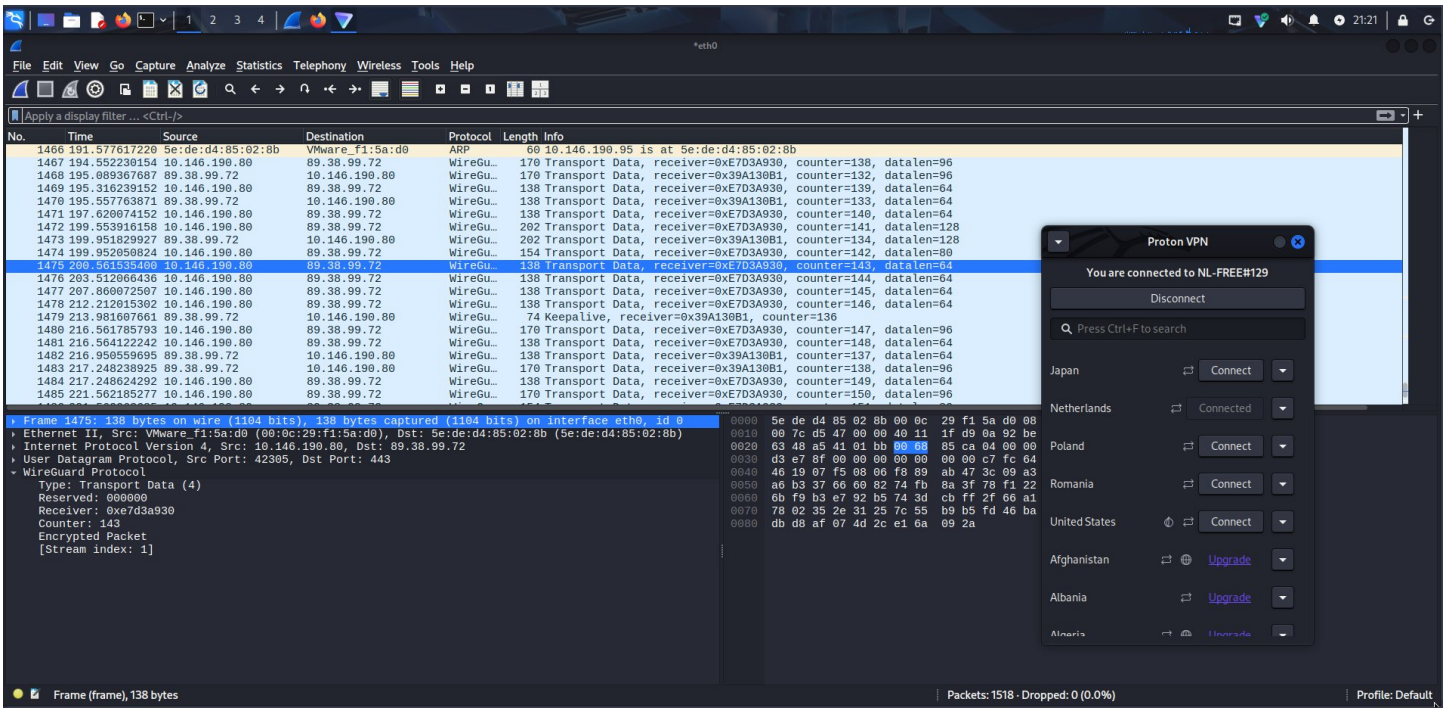
Lets see the ipaddress of the machine now , if you see the interface **eth0** the ip is 10.146.190.80, but the ip address assigned by VPN is identified in interface **proton0** with 10.2.0.2



Lets check the whatismyipaddress, to confirm the change of ip and location for confirmation



there you can see that it is connected to the Netherlands with state zuid-holland region, now lets ensure wether the traffic is being encrypt or not



To verify the Encryption we start the packet capturing tool wireshark before start of VPN, from the time i start the VPN, it is started communication in **WireGuard** protocol in UDP

What is WireGuard?

WireGuard is a modern VPN protocol designed to be fast, simple, and highly secure. It uses state-of-the-art cryptography like ChaCha20 for encryption and Poly1305 for authentication.

VPN security and encryption features

Here's a clear and up-to-date breakdown of **ProtonVPN's encryption and privacy features**, drawing from trusted reviews, official sources, and user insights:

Encryption & Protocols

- **Strong industry-standard encryption**: ProtonVPN uses **AES-256** when you're connected via OpenVPN or IKEv2, and **ChaCha20** with WireGuard—both top-tier, widely trusted algorithms.
- **Secure key management**: They implement **Perfect Forward Secrecy**, with key exchanges like RSA-4096 and HMAC-SHA-384 ensuring each session is uniquely protected.
- **Stealth protocol**: Available on newer clients (Windows, macOS, iOS, Android), this obfuscated version of WireGuard runs over TLS, masking the fact you're using a VPN—helpful in censorship-heavy regions.

Server Security & Infrastructure

- **Full-disk encryption** on all servers ensures that, even if a server is physically seized, no user data can be accessed.
- **Secure Core (multi-hop)**: Traffic is routed through multiple servers (typically in privacy-friendly nations like Switzerland, Iceland, Sweden) before exiting, guarding against network-level tracking or surveillance.
- **Server ownership and audits**: While Proton owns its Secure Core servers, others may be hosted via bare-metal third parties—always encrypted and under strict no-logs policy.

Privacy Guarantees

- **No-logs policy**: ProtonVPN doesn't store your internet activity, usage, or session data. This is reinforced by **independent audits**, with the latest from Securitum in July 2024.
- **Privacy-friendly jurisdiction**: Based in Switzerland, Proton benefits from some of the strongest privacy laws in the world, outside of surveillance coalitions like the Five Eyes.

Leak Protection & Connectivity Safety

- **DNS leak protection** and an effective **kill switch** are standard—keeping your true IP hidden even during connection drops.
- **Transparency**: Proton open-sourced all their apps in 2020 and regularly conducts external security audits.

Summary:

VPN (Virtual Private Network) enhances privacy and security by encrypting your internet traffic, hiding your IP address, and protecting against tracking, data theft, and ISP surveillance. It can bypass geo-restrictions, access censored content, and provide safer connections on public Wi-Fi. However, limitations include potential speed reduction due to encryption overhead, possible connection drops, reliance on the provider's trustworthiness, and the fact that it cannot protect against all threats like phishing or malware outside the VPN tunnel.