**Task 8 :Working with VPNs**

1.Choose a reputable free VPN service and sign up.

2.Download and install the VPN client.

3.Connect to a VPN server (choose closest or any location).

4.Verify your IP address has changed (use whatismyipaddress.com).

5.Browse a website to confirm traffic is encrypted.

6.Disconnect VPN and compare browsing speed and IP.

7.Research VPN encryption and privacy features.

8.Write a summary on VPN benefits and limitations.

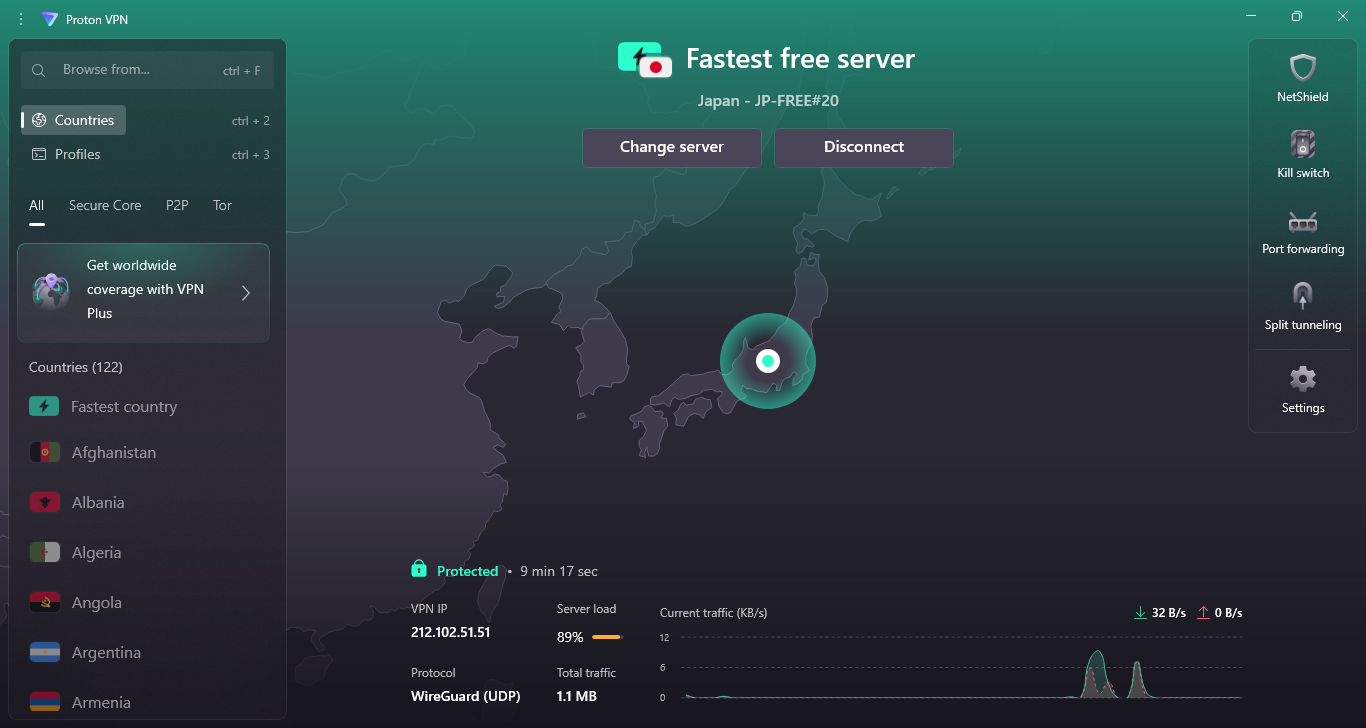
1. **Choose a reputable free VPN service and sign up.**

**PROTON VPN**

1. **Download and install the VPN client.**
2. **Connect to a VPN server (choose closest or any location)**

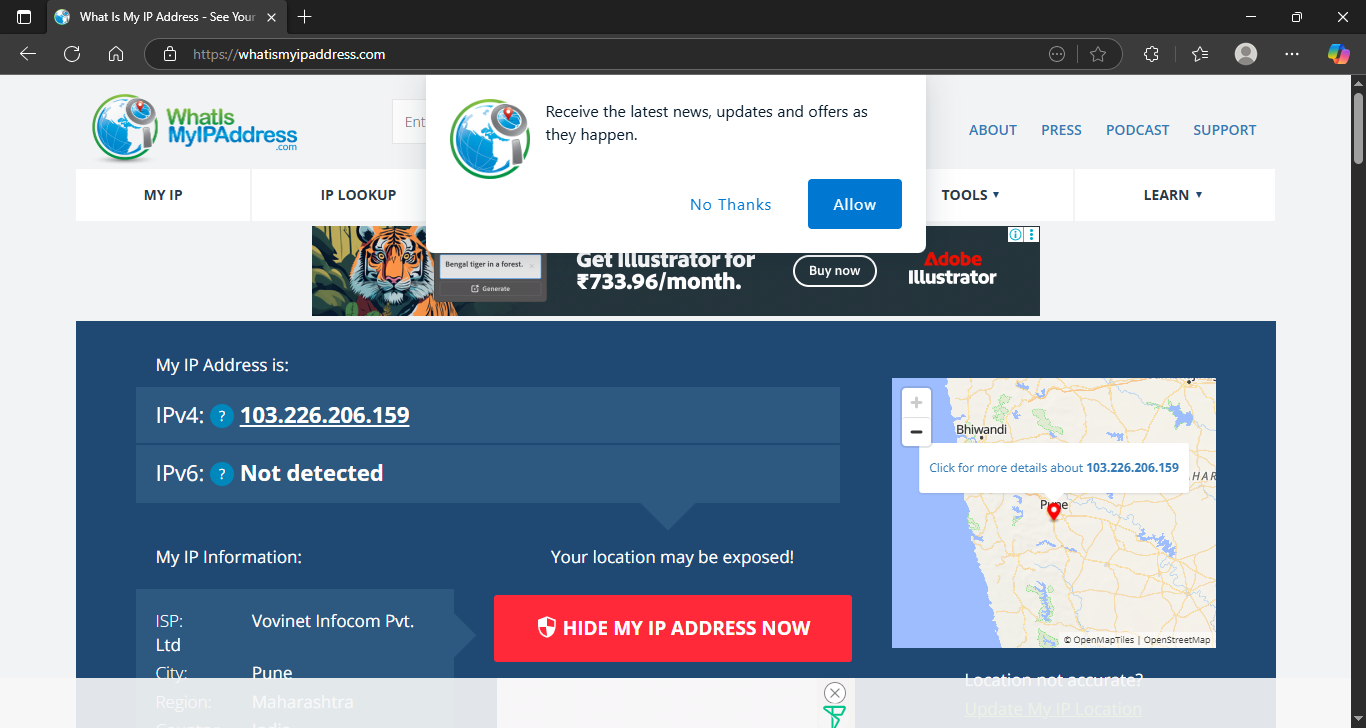
**Japan**

**Proton VPN**

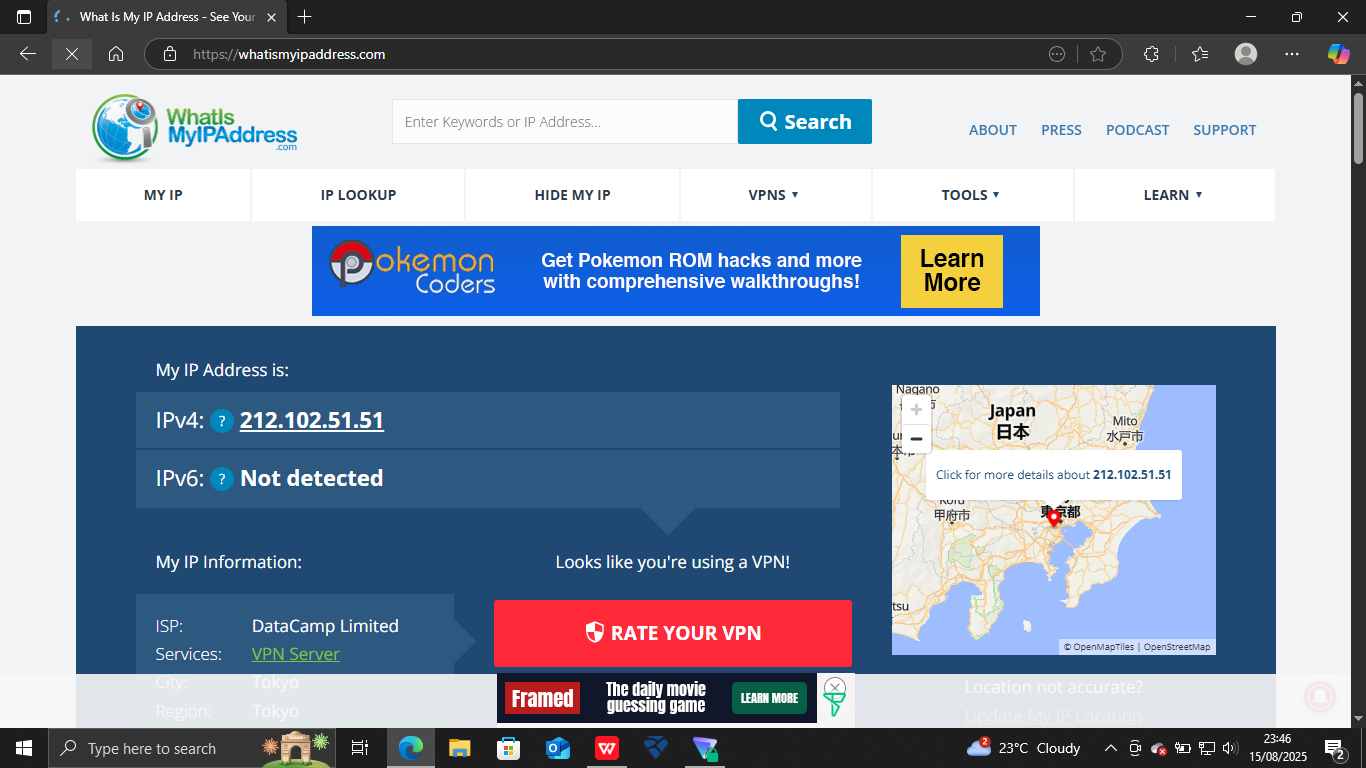
****

**4.Verify your IP address has changed (use whatismyipaddress.com).**

**Before Using VPN**



**After Using VPN**



Both of the ips are differents

**7.Research VPN encryption and privacy features.**

1. VPN Encryption Basics

Encryption is the process of converting readable data (plaintext) into an unreadable format (ciphertext) so unauthorized parties can’t interpret it.

**How It Works in a VPN**

When you connect to a VPN, your internet traffic first goes through an encrypted “tunnel.”

This encryption is handled by cryptographic algorithms.

Only the VPN server (and your device) has the keys to decrypt the data.

Example:

Without VPN → Data travels in plain text, visible to ISPs, hackers, and governments.

With VPN → Data is scrambled; even if intercepted, it looks like gibberish.

**a. No-Logs Policy**

The VPN doesn’t store your browsing history, IP address, or connection timestamps.

Independent audits by third parties can verify this claim.

**b. IP Address Masking**

Your real IP address is replaced with the VPN server’s IP.

Websites, trackers, and even your ISP see the VPN server’s location, not yours.

**c. DNS Leak Protection**

Prevents DNS requests from bypassing the VPN tunnel and revealing your activity.

Good VPNs run their own encrypted DNS servers.

**f. Multi-Hop (Double VPN)**

Routes your connection through two VPN servers for extra anonymity.

Increases encryption layers but may slow speed.

**4. Limitations**

Not 100% anonymous — Your VPN provider could theoretically see your traffic if they keep logs.

Device security still matters — If your device is infected with malware, VPN encryption won’t help.

Traffic analysis possible — Government agencies can sometimes guess patterns even if content is encrypted.

**5. Best Practices for VPN Privacy**

Choose a VPN with strong protocols (OpenVPN or WireGuard).

Verify no-logs policy with independent audits.

Enable kill switch and DNS leak protection.

**8.Write a summary on VPN benefits and limitations.**

**VPN Benefits**

* Data Encryption – Protects your online activity from hackers, ISPs, and government surveillance.
* IP Address Masking – Hides your real location, enhancing privacy.
* Secure Public Wi-Fi Use – Prevents data theft on open networks.
* Bypass Geo-Restrictions – Access blocked websites and streaming services in other regions.
* Avoid Bandwidth Throttling – Stops ISPs from slowing your connection based on usage.
* Extra Security Features – Kill switch, DNS leak protection, and multi-hop routing add layers of safety.

**VPN Limitations**

* Not Fully Anonymous – VPN providers can see your traffic if they keep logs.
* Slower Speeds – Encryption and routing through VPN servers can reduce speed.
* No Protection Against Malware – VPNs don’t stop viruses or phishing attacks.
* Blocked by Some Websites – Some platforms actively detect and block VPN IPs.
* Trust Factor – You must trust the VPN provider with your data.
* Legal Restrictions – VPN use may be regulated or banned in certain countries.