TASK 8 : Working with VPNs

➢ Research VPN encryption and privacy features.

- **VPN Encryption Technologies :**

These define **how** data is encrypted and tunnelled through the VPN:

Protocol	Encryption	Speed	Security	Notes
OpenVPN	AES-256-GCM	Moderate	Very High	Open-source, widely audited
Wire Guard	ChaCha20-Poly1305	Very Fast	High	Modern, lean codebase
IKEv2/IPSec	AES-256	Fast	High	Great for mobile (auto-reconnect)
L2TP/IPSec	AES-128/256	Slow	Moderate	Old but still used
PPTP	MPPE (128-bit)	Fast	Very Low	Deprecated – avoid

- **VPN Privacy Features**

To protect user identity and browsing behaviour, privacy-focused VPNs include:

1. No-Logs Policy

- Means the VPN provider does **not store connection, traffic, DNS queries, or user metadata**.
- Must be backed by **independent security audits** or **warrant canaries**.
- Example: **Mullvad, ProtonVPN, IVPN** (have had audits or operate without user accounts).

---

2. Kill Switch

- Cuts off your Internet traffic if the VPN tunnel drops.
- Prevents **accidental IP/DNS leaks** during disconnects.
- Crucial for anonymity in OSINT or red team scenarios.

---

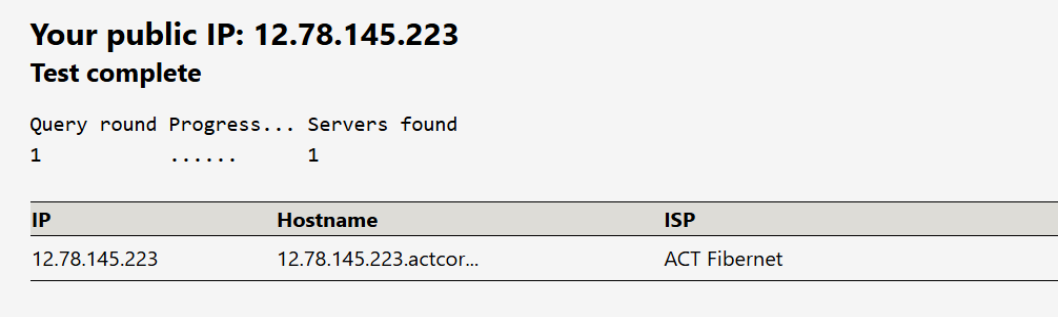
3. DNS Leak Protection

- Ensures your DNS queries are not sent to your ISP or third parties.
- Uses **encrypted DNS** or custom DNS resolvers (often DoH/DoT).

- Check via: dnsleaktest.com

  - **Using Windscribe free Vpn :**

    - Before Connect to VPN dnsleaktest :



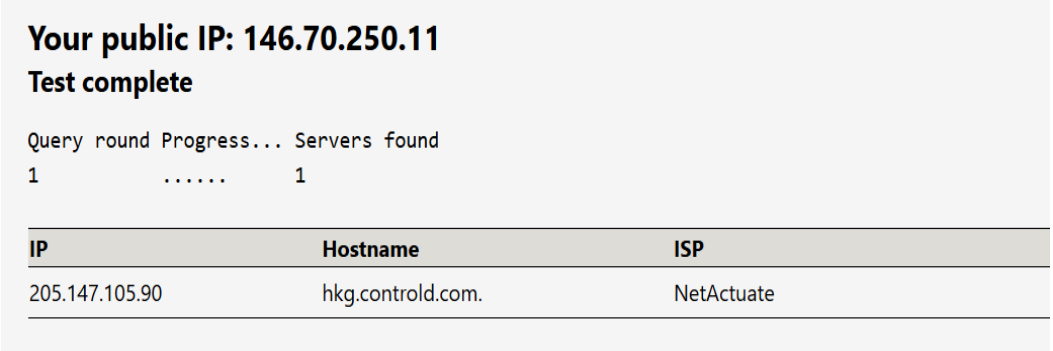
Your public IP: 12.78.145.223

Test complete

Query round Progress... Servers found
1 1

IP	Hostname	ISP
12.78.145.223	12.78.145.223.actcor...	ACT Fibernet

    - After Connect to VPN dnsleaktest :



Your public IP: 146.70.250.11

Test complete

Query round Progress... Servers found
1 1

IP	Hostname	ISP
205.147.105.90	hkg.controld.com.	NetActuate

---

4. WebRTC & IPv6 Leak Protection

- WebRTC can expose local IP addresses via browsers.
- IPv6 can leak traffic if not properly tunnelled.
- Good VPNs disable or block both.

➢ Write a summary on VPN benefits and limitations

- **VPN Benefits :**

1. **Encryption & Security**
   - Encrypts your internet traffic, protecting it from eavesdropping on public Wi-Fi or untrusted networks.
   - Shields sensitive data from attackers or network sniffers.

2. **Privacy & Anonymity**

- Masks your real IP address, making it harder for websites, ISPs, or government entities to track your online activity.
- Prevents DNS leaks when properly configured.

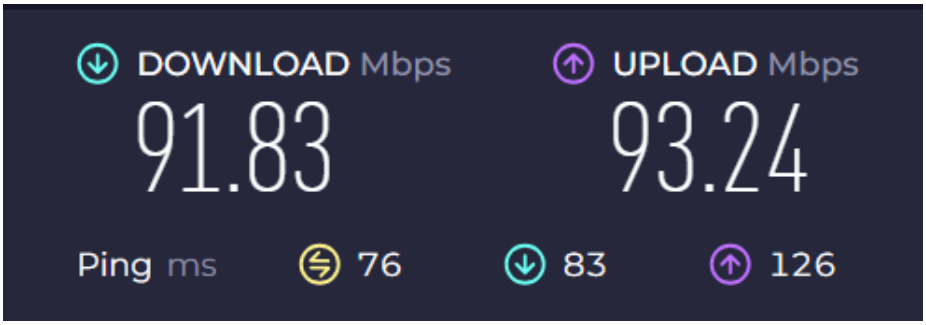
3. **Remote Access**
   - Securely access internal company networks or lab environments from anywhere.
   - Common in enterprise environments for secure remote work.

4. **Bypass Censorship & Geo-Restrictions**
   - Access blocked websites and services in restricted regions (e.g., streaming platforms, news sites, social media).
   - Useful in countries with strict Internet controls (e.g., China, Iran).

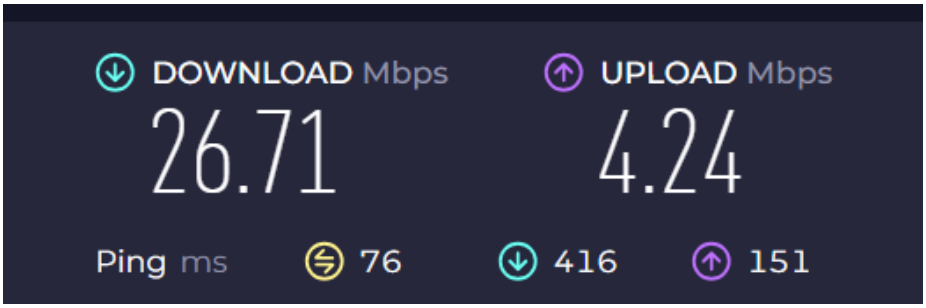
- **<u>Limitations of VPNs</u> :**

1. **Not Total Anonymity**
   - VPNs don't anonymize like Tor; the provider can still see your traffic origin unless they have a strict no-logs policy.
   - If the VPN is compromised or subpoenaed (and logs exist), your identity could be revealed.

2. **Performance Impact**
   - Encryption overhead and routing through distant servers can reduce speed.
   - Some free VPNs have strict bandwidth or speed limitations.
   - Before Connect to VPN Internet speed :



   - After connect to VPN internet speed:



3. **Blocked by Some Services**
    - Many platforms (Netflix, banking, government portals) detect and block known VPN IPs.
    - May require rotating servers or obfuscation features to bypass.

4. **False Sense of Security**
    - VPNs don’t protect against **malware**, **phishing**, or **browser fingerprinting**.

5. **Free VPN Risks**
    - Free VPNs may log and sell your data, inject ads, or operate insecure infrastructure.
    - Some are outright malicious (e.g., Hola VPN's past incidents).