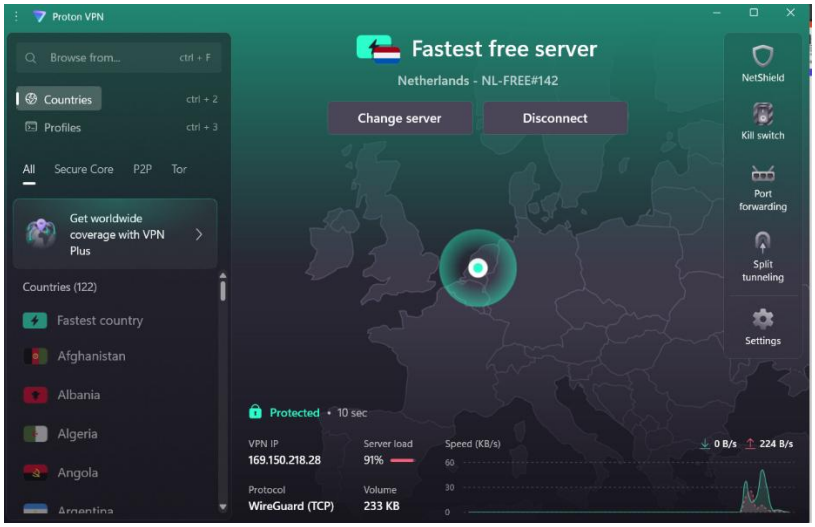
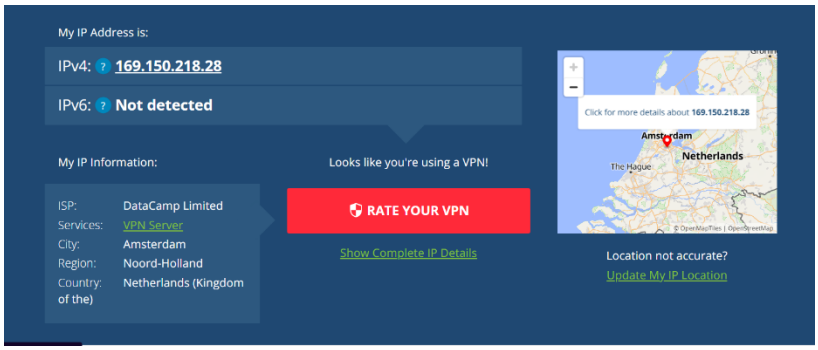
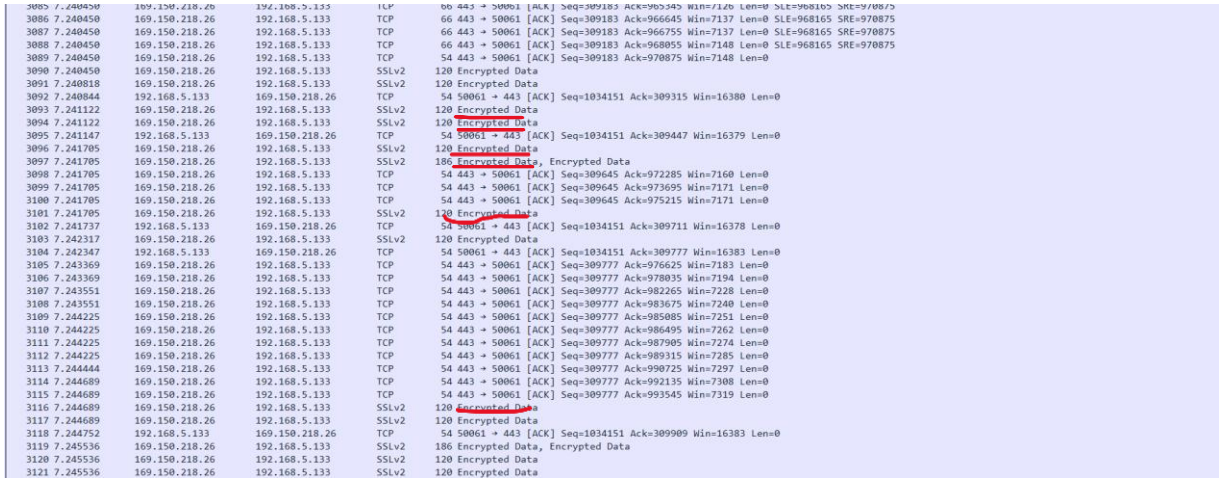


Connected to the proton vpn and it has changed my ip and I confirmed it in whatismyipaddress.com



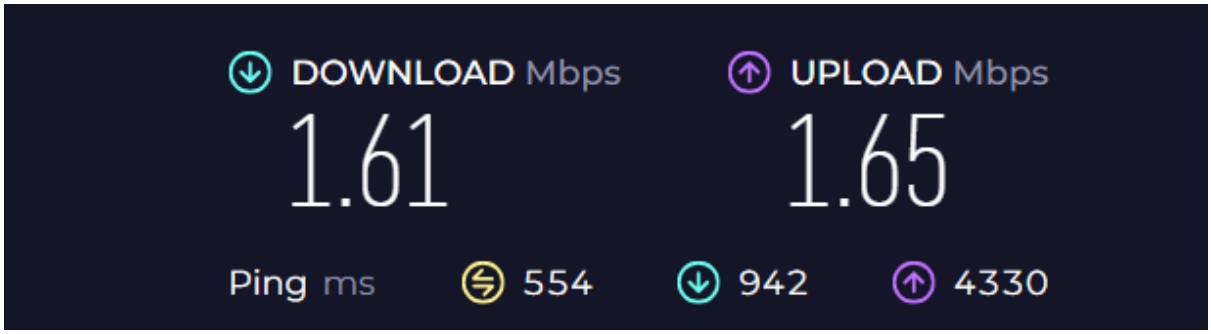
And checked the traffic when connected to the vpn and confirmed that the traffic is encrypted



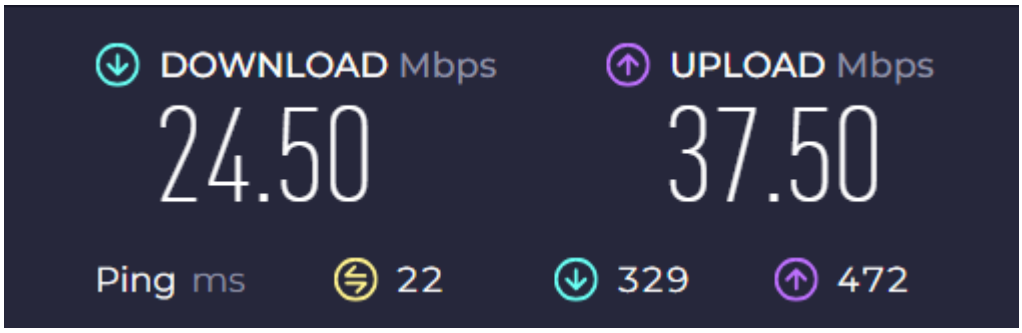
3086	7.240450	169.150.218.26	192.168.5.133	TCP	66 443 → 50061 [ACK] Seq=309183 Ack=966645 Win=7137 Len=0 SLE=968165 SRE=970875
3087	7.240450	169.150.218.26	192.168.5.133	TCP	66 443 → 50061 [ACK] Seq=309183 Ack=966755 Win=7137 Len=0 SLE=968165 SRE=970875
3088	7.240450	169.150.218.26	192.168.5.133	TCP	66 443 → 50061 [ACK] Seq=309183 Ack=968055 Win=7148 Len=0 SLE=968165 SRE=970875
3089	7.240450	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309183 Ack=970875 Win=7148 Len=0
3090	7.240450	169.150.218.26	192.168.5.133	SSLv2	120 Encrypted Data
3091	7.240818	169.150.218.26	192.168.5.133	SSLv2	120 Encrypted Data
3092	7.240844	192.168.5.133	169.150.218.26	TCP	54 50061 → 443 [ACK] Seq=1034151 Ack=309315 Win=16380 Len=0
3093	7.241122	169.150.218.26	192.168.5.133	SSLv2	120 Encrypted Data
3094	7.241122	169.150.218.26	192.168.5.133	SSLv2	120 Encrypted Data
3095	7.241147	192.168.5.133	169.150.218.26	TCP	54 50061 → 443 [ACK] Seq=1034151 Ack=309447 Win=16379 Len=0
3096	7.241705	169.150.218.26	192.168.5.133	SSLv2	120 Encrypted Data
3097	7.241705	169.150.218.26	192.168.5.133	SSLv2	186 Encrypted Data, Encrypted Data
3098	7.241705	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309645 Ack=972285 Win=7160 Len=0
3099	7.241705	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309645 Ack=973695 Win=7171 Len=0
3100	7.241705	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309645 Ack=975215 Win=7171 Len=0
3101	7.241705	169.150.218.26	192.168.5.133	SSLv2	120 Encrypted Data
3102	7.241737	192.168.5.133	169.150.218.26	TCP	54 50061 → 443 [ACK] Seq=1034151 Ack=309711 Win=16378 Len=0
3103	7.242317	169.150.218.26	192.168.5.133	SSLv2	120 Encrypted Data
3104	7.242347	192.168.5.133	169.150.218.26	TCP	54 50061 → 443 [ACK] Seq=1034151 Ack=309777 Win=16383 Len=0
3105	7.243369	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309777 Ack=976625 Win=7183 Len=0
3106	7.243369	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309777 Ack=978035 Win=7194 Len=0
3107	7.243551	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309777 Ack=982265 Win=7228 Len=0
3108	7.243551	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309777 Ack=983675 Win=7240 Len=0
3109	7.244225	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309777 Ack=985085 Win=7251 Len=0
3110	7.244225	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309777 Ack=986495 Win=7262 Len=0
3111	7.244225	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309777 Ack=987905 Win=7274 Len=0
3112	7.244225	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309777 Ack=989315 Win=7285 Len=0
3113	7.244444	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309777 Ack=990725 Win=7297 Len=0
3114	7.244689	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309777 Ack=992135 Win=7308 Len=0
3115	7.244689	169.150.218.26	192.168.5.133	TCP	54 443 → 50061 [ACK] Seq=309777 Ack=993545 Win=7319 Len=0
3116	7.244689	169.150.218.26	192.168.5.133	SSLv2	120 Encrypted Data
3117	7.244689	169.150.218.26	192.168.5.133	SSLv2	120 Encrypted Data
3118	7.244752	192.168.5.133	169.150.218.26	TCP	54 50061 → 443 [ACK] Seq=1034151 Ack=309909 Win=16383 Len=0
3119	7.245536	169.150.218.26	192.168.5.133	SSLv2	186 Encrypted Data, Encrypted Data
3120	7.245536	169.150.218.26	192.168.5.133	SSLv2	120 Encrypted Data
3121	7.245536	169.150.218.26	192.168.5.133	SSLv2	120 Encrypted Data

Speed changes when connected to vpn and feels faster without vpn

With vpn:



Without vpn:



Ip changed when disconnected vpn

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.5.133
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.5.164
```

VPN Encryption:

- VPNs use strong encryption algorithms like **AES-256** to secure your internet traffic.
- VPN protocols such as **OpenVPN**, **WireGuard**, and **IKEv2/IPSec** create an **encrypted tunnel** between your device and the VPN server.
- This tunnel ensures that even if someone intercepts the data, they **cannot read or tamper with it**.

Privacy Features:

- **IP Address Masking**: Hides your real IP address and replaces it with the VPN server's IP.
- **No-logs Policy**: Trusted VPNs don't store browsing data or connection logs.
- **Kill Switch**: Disconnects internet access if the VPN drops, preventing data leaks.
- **DNS Leak Protection**: Ensures DNS queries go through the encrypted tunnel.
- **Split Tunneling**: Lets you choose which apps use the VPN and which don't.

Summary: VPN Benefits and Limitations

Benefits:

- **Encrypts internet traffic**, protecting data from hackers and snooping.
- **Hides your IP address**, improving anonymity.
- **Accesses geo-blocked content**, such as streaming services or restricted websites.
- **Protects on public Wi-Fi**, such as in cafes or airports.
- **Bypasses censorship**, useful in restricted regions.

Limitations:

- **Slower speeds** due to encryption overhead and server distance.
- **Not 100% anonymous**—VPNs can still log or be compelled to share data.
- **May be blocked** by some websites or streaming services.
- **Free VPNs** often come with poor security, ads, or sell user data.
- **Doesn't protect from malware** unless bundled with security features.