Working with VPNs

Step 1 Prepare ProtonVPN for Use on Windows

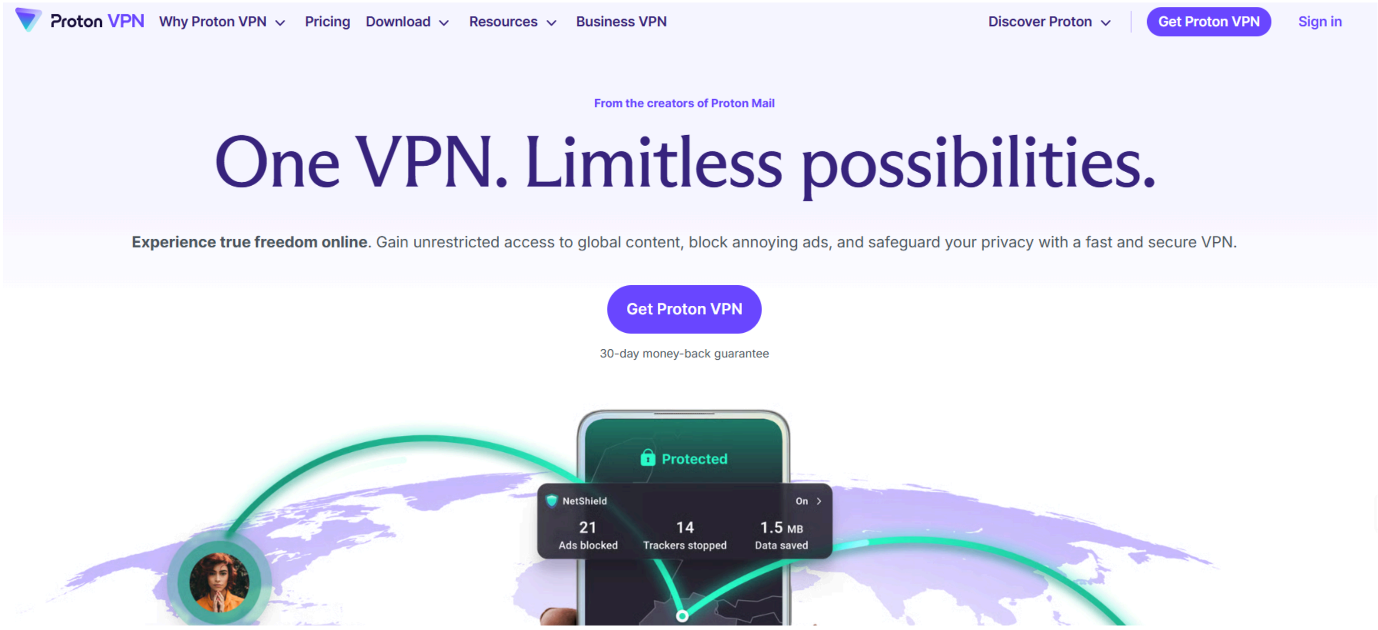
1. Open your browser and go to **https://protonvpn.com**.

2. Log in to your existing **ProtonVPN** account.

3. Make sure you are on the **Free Plan** (check under *Dashboard* > *Plans*).

4. Download the **ProtonVPN Windows client** from the official website (*Download* > *Windows*).

5. Once the .exe file is downloaded, keep it ready for installation



From the creators of Proton Mail

One VPN. Limitless possibilities.

Experience true freedom online. Gain unrestricted access to global content, block annoying ads, and safeguard your privacy with a fast and secure VPN.

30-day money-back guarantee

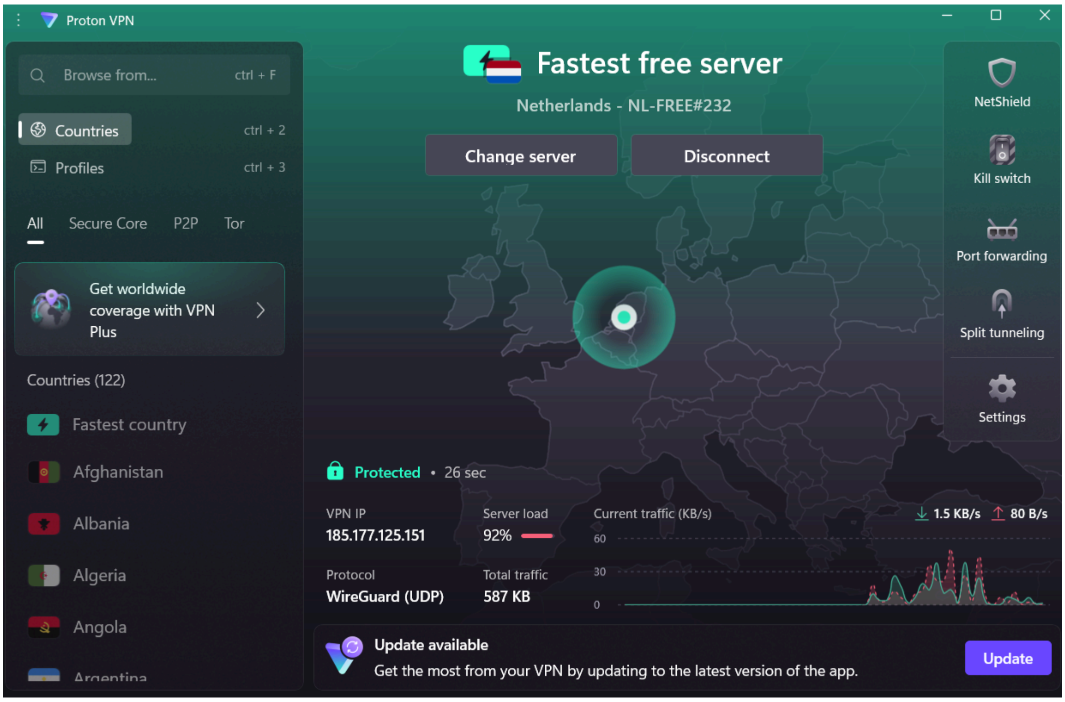
VPN Concept Note for this step:

- ProtonVPN will create an **encrypted tunnel** between your device and a VPN server.

- This tunnel hides your real IP address, protecting **privacy** and securing communication against interception on untrusted networks.

Step 2 Install and Connect to ProtonVPN on Windows

1. **Install the VPN Client**
   - Double-click the downloaded **ProtonVPN Windows installer (.exe)**.
   - Follow the installation wizard:
     - Accept the license agreement.
     - Choose the default installation location (unless you need to change it).
     - Click **Install** and wait for it to complete.
   - Once installed, launch **ProtonVPN**.
2. **Log In**
   - Enter your ProtonVPN username and password.
   - If 2FA is enabled, enter your verification code.
3. **Connect to a VPN Server**
   - In the ProtonVPN dashboard, switch to the **Countries** tab.
   - Pick any **Free server** (marked with a green “Free” label).
   - Click **Connect**.
   - Wait until the status shows **Connected** and a new IP address appears.



Fastest free server

Netherlands - NL-FREE#232

Protected • 26 sec

VPN IP 185.177.125.151

Server load 92%

Protocol WireGuard (UDP)

Total traffic 587 KB

Current traffic (KB/s) ↓ 1.5 KB/s ↑ 80 B/s

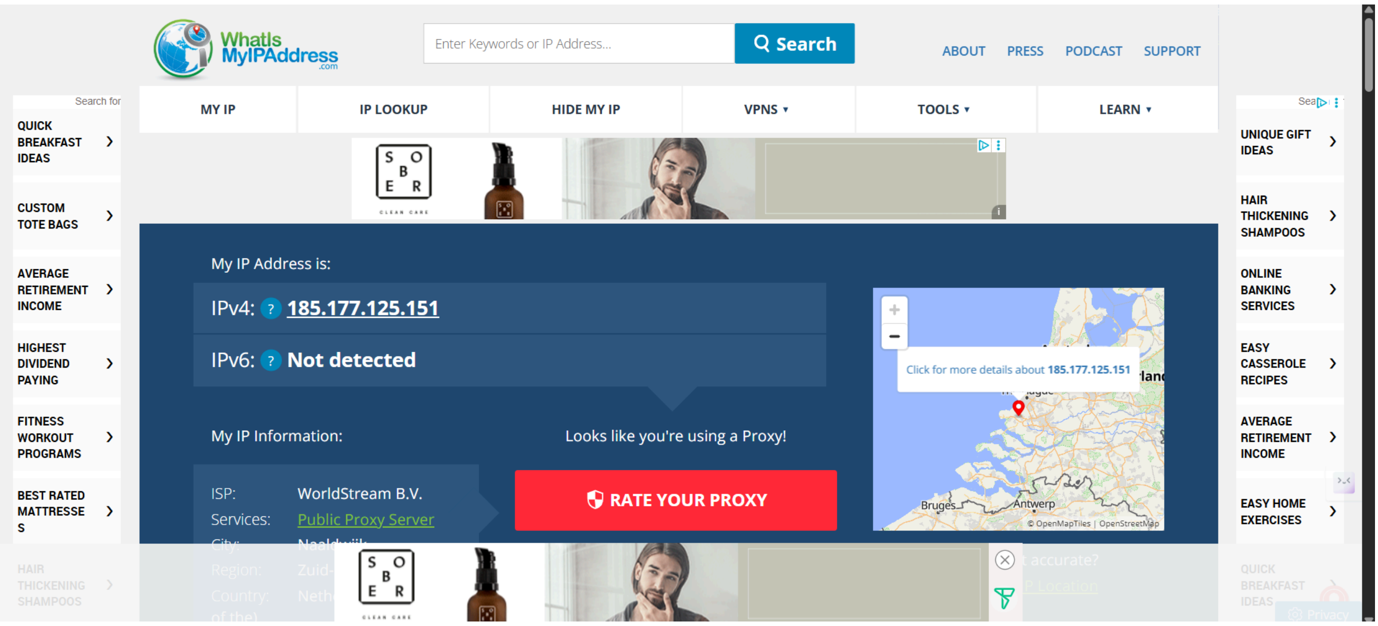
Update available

Get the most from your VPN by updating to the latest version of the app.

4. **Verify the Connection**

    ○ Open a browser and visit https://whatismyipaddress.com/.

    ○ Confirm that the IP shown matches the VPN server location, not your real location.



My IP Address is:

IPv4: 185.177.125.151

IPv6: Not detected

My IP Information:

Looks like you're using a Proxy!

ISP: WorldStream B.V.
Services: Public Proxy Server
City: Naaldwijk
Region: Zuid-
Country: Neth

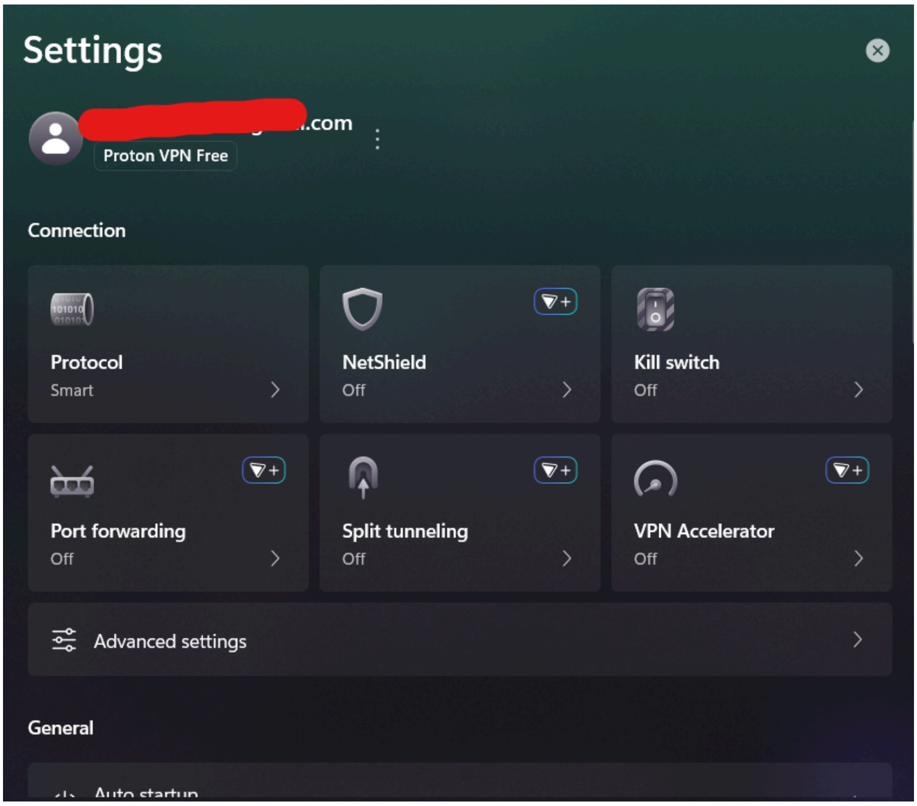
VPN Concept Note for this step:

- When you connect, ProtonVPN uses **tunneling protocols** (like OpenVPN or WireGuard) to encapsulate your traffic inside an **encrypted channel**.
- This prevents data interception, boosting **network security**.

Step 3 Test Encryption & Identify the Tunneling Protocol

1. **Check ProtonVPN's Protocol**

    - In the ProtonVPN app, go to **Settings > Connection**.
    - Look for the **VPN Protocol** option; it should say something like **OpenVPN (UDP/TCP)** or **WireGuard**.
    - Note which one is being used right now.



Settings

[redacted].com

Proton VPN Free

Connection

Protocol
Smart

NetShield
Off

Kill switch
Off

Port forwarding
Off

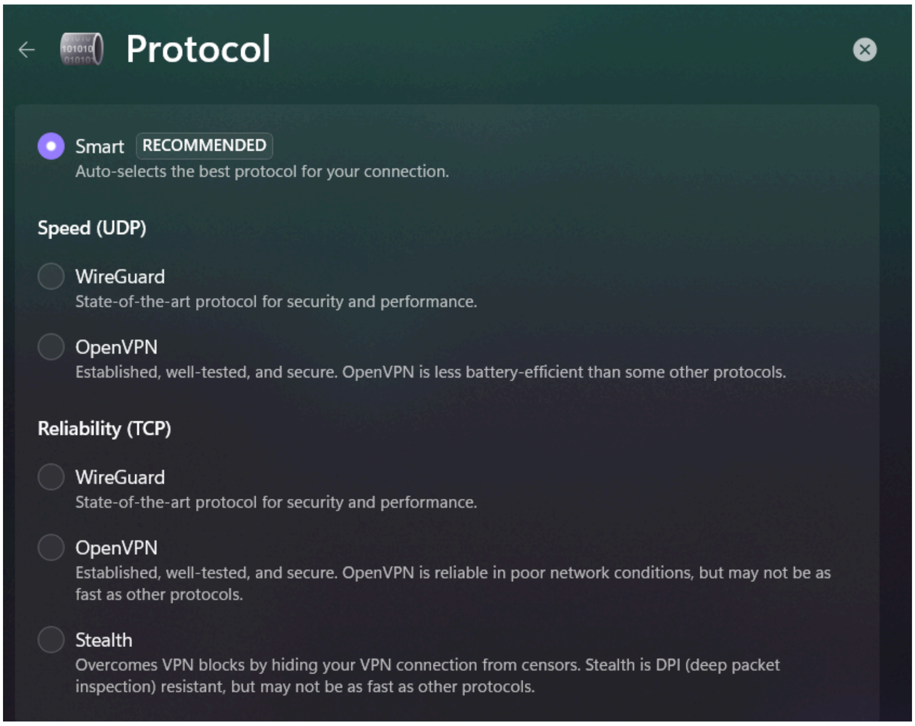
Split tunneling
Off

VPN Accelerator
Off

Advanced settings

General

Auto startup



Protocol

● Smart RECOMMENDED
Auto-selects the best protocol for your connection.

Speed (UDP)

○ WireGuard
State-of-the-art protocol for security and performance.

○ OpenVPN
Established, well-tested, and secure. OpenVPN is less battery-efficient than some other protocols.

Reliability (TCP)

○ WireGuard
State-of-the-art protocol for security and performance.

○ OpenVPN
Established, well-tested, and secure. OpenVPN is reliable in poor network conditions, but may not be as fast as other protocols.

○ Stealth
Overcomes VPN blocks by hiding your VPN connection from censors. Stealth is DPI (deep packet inspection) resistant, but may not be as fast as other protocols.

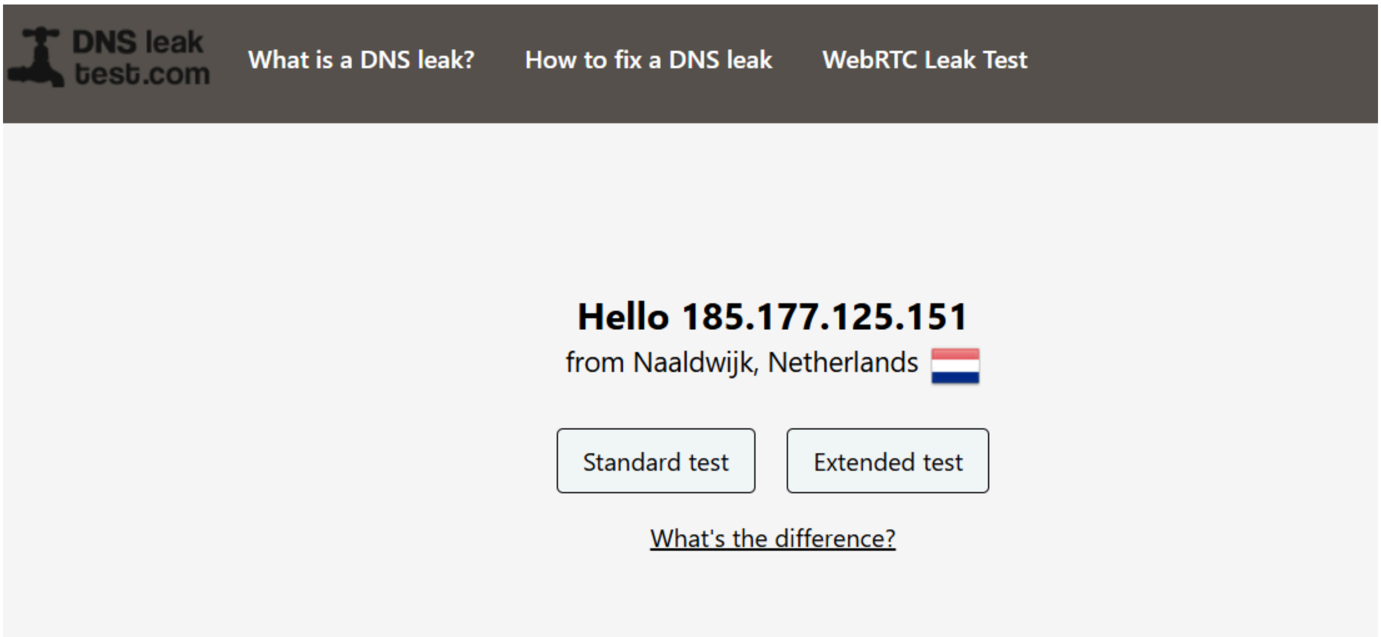
2. **Test Data Encryption**

   ○ Open your browser and go to **https://www.dnsleaktest.com/**.

   ○ Click **Standard Test**.

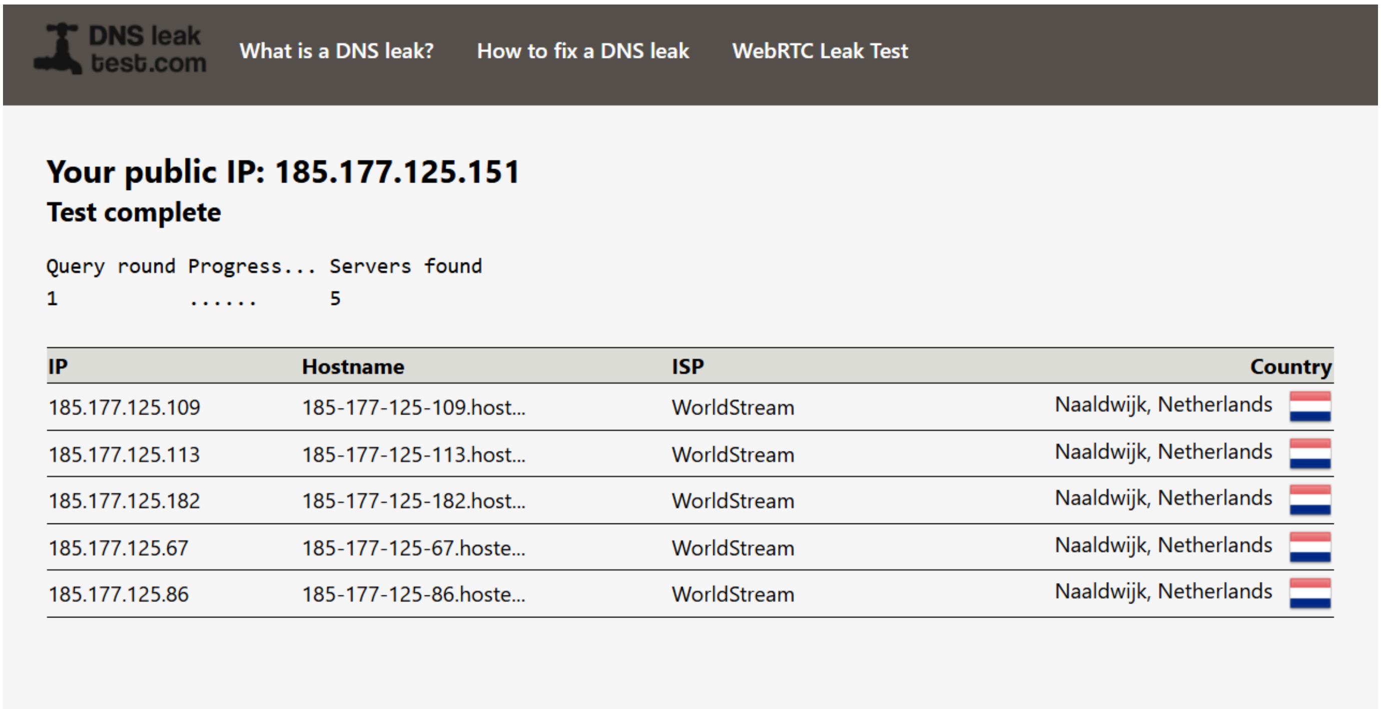
   ○ Verify that the DNS servers listed match your VPN's country (Netherlands) and not your real ISP's servers.

   ○ This confirms that DNS queries are also going through the encrypted tunnel.



Hello 185.177.125.151

from Naaldwijk, Netherlands



Your public IP: 185.177.125.151

Test complete

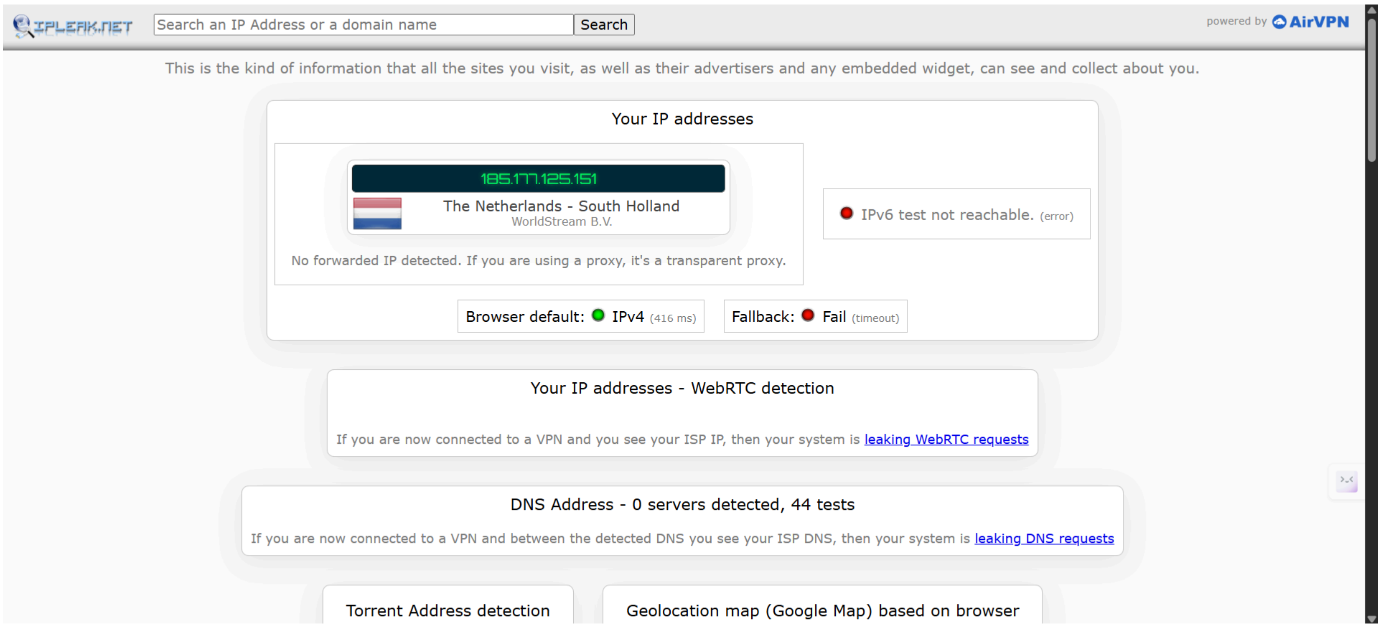
```
Query round Progress... Servers found
1           ......      5
```

IP	Hostname	ISP	Country
185.177.125.109	185-177-125-109.host...	WorldStream	Naaldwijk, Netherlands
185.177.125.113	185-177-125-113.host...	WorldStream	Naaldwijk, Netherlands
185.177.125.182	185-177-125-182.host...	WorldStream	Naaldwijk, Netherlands
185.177.125.67	185-177-125-67.hoste...	WorldStream	Naaldwijk, Netherlands
185.177.125.86	185-177-125-86.hoste...	WorldStream	Naaldwijk, Netherlands

3. **Extra Privacy Check**

    ○ Visit **https://ipleak.net/**.

    ○ Confirm that your **IPv4**, **IPv6** (if any), and DNS information all reflect the VPN server location, not your own.



This is the kind of information that all the sites you visit, as well as their advertisers and any embedded widget, can see and collect about you.

Your IP addresses

185.177.125.151

The Netherlands - South Holland

WorldStream B.V.

No forwarded IP detected. If you are using a proxy, it's a transparent proxy.

● IPv6 test not reachable. (error)

Browser default: ● IPv4 (416 ms)

Fallback: ● Fail (timeout)

Your IP addresses - WebRTC detection

If you are now connected to a VPN and you see your ISP IP, then your system is leaking WebRTC requests

DNS Address - 0 servers detected, 44 tests

If you are now connected to a VPN and between the detected DNS you see your ISP DNS, then your system is leaking DNS requests

Torrent Address detection

Geolocation map (Google Map) based on browser

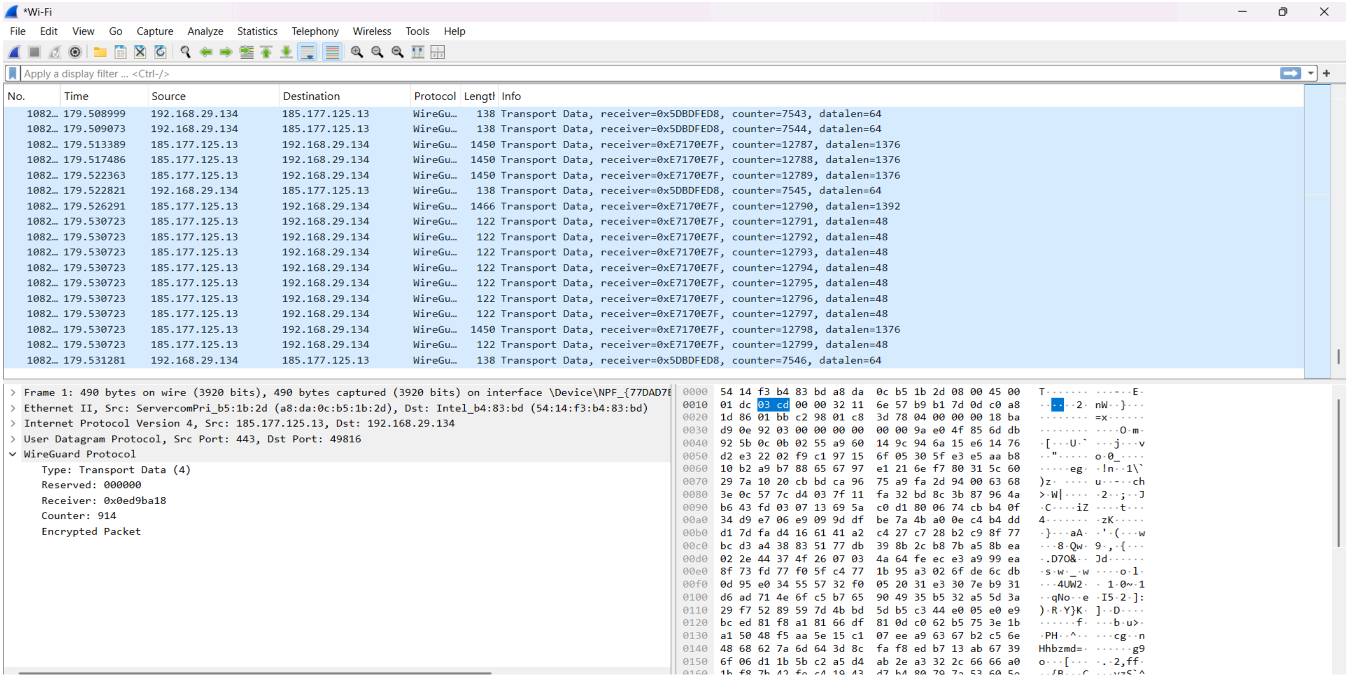
VPN Concept Note for this step:

- **Encryption:** VPN protocols use ciphers (e.g., AES-256) to make intercepted data unreadable.
- **Tunneling:** OpenVPN and WireGuard wrap your traffic into a secure “tunnel,” preventing outsiders from seeing what you send or receive.

Step 4 Demonstrate VPN Protection Against Traffic Interception

We'll simulate what an attacker might see **with VPN on** vs **without VPN**, using Wireshark on Windows.

1. **Install Wireshark** (if not already installed)
    - Download from: https://www.wireshark.org/download.html
    - Install with default settings.
    - Allow installation of WinPcap or Npcap when prompted (required for packet capture).
2. **Capture Traffic With VPN ON**
    - Ensure ProtonVPN is **connected** to the Netherlands server.
    - Open Wireshark and select your active network interface (usually Wi-Fi or Ethernet).
    - Click **Start Capturing Packets**.
    - Browse a few websites (e.g., example.com, wikipedia.org).
    - Stop the capture after 1–2 minutes.
    - Look at the **Protocol** column; ProtonVPN is using **WireGuard** as its tunneling protocol.
    - All your traffic is being wrapped inside **WireGuard UDP packets**, which are encrypted with **ChaCha20** cipher and authenticated with Poly1305 (very strong, modern cryptography).



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.      Time        Source           Destination      Protocol Lengtl Info
   1082… 179.508999  192.168.29.134   185.177.125.13   WireGu…    138 Transport Data, receiver=0x5DBDFED8, counter=7543, datalen=64
   1082… 179.509073  192.168.29.134   185.177.125.13   WireGu…    138 Transport Data, receiver=0x5DBDFED8, counter=7544, datalen=64
   1082… 179.513389  185.177.125.13   192.168.29.134   WireGu…   1450 Transport Data, receiver=0xE7170E7F, counter=12787, datalen=1376
   1082… 179.517486  185.177.125.13   192.168.29.134   WireGu…   1450 Transport Data, receiver=0xE7170E7F, counter=12788, datalen=1376
   1082… 179.522363  185.177.125.13   192.168.29.134   WireGu…   1450 Transport Data, receiver=0xE7170E7F, counter=12789, datalen=1376
   1082… 179.522821  192.168.29.134   185.177.125.13   WireGu…    138 Transport Data, receiver=0x5DBDFED8, counter=7545, datalen=64
   1082… 179.526291  185.177.125.13   192.168.29.134   WireGu…   1466 Transport Data, receiver=0xE7170E7F, counter=12790, datalen=1392
   1082… 179.530723  185.177.125.13   192.168.29.134   WireGu…    122 Transport Data, receiver=0xE7170E7F, counter=12791, datalen=48
   1082… 179.530723  185.177.125.13   192.168.29.134   WireGu…    122 Transport Data, receiver=0xE7170E7F, counter=12792, datalen=48
   1082… 179.530723  185.177.125.13   192.168.29.134   WireGu…    122 Transport Data, receiver=0xE7170E7F, counter=12793, datalen=48
   1082… 179.530723  185.177.125.13   192.168.29.134   WireGu…    122 Transport Data, receiver=0xE7170E7F, counter=12794, datalen=48
   1082… 179.530723  185.177.125.13   192.168.29.134   WireGu…    122 Transport Data, receiver=0xE7170E7F, counter=12795, datalen=48
   1082… 179.530723  185.177.125.13   192.168.29.134   WireGu…    122 Transport Data, receiver=0xE7170E7F, counter=12796, datalen=48
   1082… 179.530723  185.177.125.13   192.168.29.134   WireGu…    122 Transport Data, receiver=0xE7170E7F, counter=12797, datalen=48
   1082… 179.530723  185.177.125.13   192.168.29.134   WireGu…   1450 Transport Data, receiver=0xE7170E7F, counter=12798, datalen=1376
   1082… 179.530723  185.177.125.13   192.168.29.134   WireGu…    122 Transport Data, receiver=0xE7170E7F, counter=12799, datalen=48
   1082… 179.531281  192.168.29.134   185.177.125.13   WireGu…    138 Transport Data, receiver=0x5DBDFED8, counter=7546, datalen=64
```

```
> Frame 1: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits) on interface \Device\NPF_{77DAD7E
> Ethernet II, Src: ServercomPri_b5:1b:2d (a8:da:0c:b5:1b:2d), Dst: Intel_b4:83:bd (54:14:f3:b4:83:bd)
> Internet Protocol Version 4, Src: 185.177.125.13, Dst: 192.168.29.134
> User Datagram Protocol, Src Port: 443, Dst Port: 49816
v WireGuard Protocol
    Type: Transport Data (4)
    Reserved: 000000
    Receiver: 0x0ed9ba18
    Counter: 914
    Encrypted Packet
```

```
0000  54 14 f3 b4 83 bd a8 da  0c b5 1b 2d 08 00 45 00   T·······  ···-··E·
0010  01 dc 03 cd 00 00 32 11  6e 57 b9 b1 7d 0d c0 a8   ······2·  nW··}···
0020  1d 86 01 bb c2 98 01 c8  3d 78 04 00 00 00 18 ba   ········  =x······
0030  d9 0e 92 03 00 00 00 00  00 00 9a e0 4f 85 6d db   ········  ····O·m·
0040  92 5b 0c 0b 02 55 a9 60  14 9c 94 6a 15 e6 14 76   ·[···U·`  ···j···v
0050  d2 e3 22 02 f9 c1 97 15  6f 05 30 5f e3 e5 aa b8   ··"·····  o·0_····
0060  10 b2 a9 b7 88 65 67 97  e1 21 6e f7 80 31 5c 60   ·····eg·  ·!n··1\`
0070  29 7a 10 20 cb bd ca 96  75 a9 fa 2d 94 00 63 68   )z· ····  u··-··ch
0080  3e 0c 57 7c d4 03 7f 11  fa 32 bd 8c 3b 87 96 4a   >·W|····  ·2··;··J
0090  b6 43 fd 03 07 13 69 5a  c0 d1 80 06 74 cb b4 0f   ·C····iZ  ····t···
00a0  34 d9 e7 06 e9 09 9d df  be 7a 4b a0 0e c4 b4 dd   4·······  ·zK·····
00b0  d1 7d fa d4 16 61 41 a2  c4 27 c7 28 b2 c9 8f 77   ·}···aA·  ·'·(···w
00c0  bc d3 a4 38 83 51 77 db  39 8b 2c b8 7b a5 8b ea   ···8·Qw·  9·,·{···
00d0  02 2e 44 37 4f 26 07 03  4a 64 fe ec e3 a9 99 ea   ·.D7O&··  Jd······
00e0  8f 73 fd 77 f0 5f c4 77  1b 95 a3 02 6f de 6c db   ·s·w·_·w  ····o·l·
00f0  0d 95 e0 34 55 57 32 f0  05 20 31 e3 30 7e b9 31   ···4UW2·  · 1·0~·1
0100  d6 ad 71 4e 6f c5 b7 65  90 49 35 b5 32 a5 5d 3a   ··qNo··e  ·I5·2·]:
0110  29 f7 52 89 59 7d 4b bd  5d b5 c3 44 e0 05 e0 e9   )·R·Y}K·  ]··D····
0120  bc ed 81 f8 a1 81 66 df  81 0d c0 62 b5 75 3e 1b   ······f·  ···b·u>·
0130  a1 50 48 f5 aa 5e 15 c1  07 ee a9 63 67 b2 c5 6e   ·PH··^··  ···cg··n
0140  48 68 62 7a 6d 64 3d 8c  fa f8 ed b7 13 ab 67 39   Hhbzmd=·  ······g9
0150  6f 06 d1 1b 5b c2 a5 d4  ab 2e a3 32 2c 66 66 a0   o···[···  ·.·2,ff·
```

3. **Capture Traffic With VPN OFF** (for comparison)

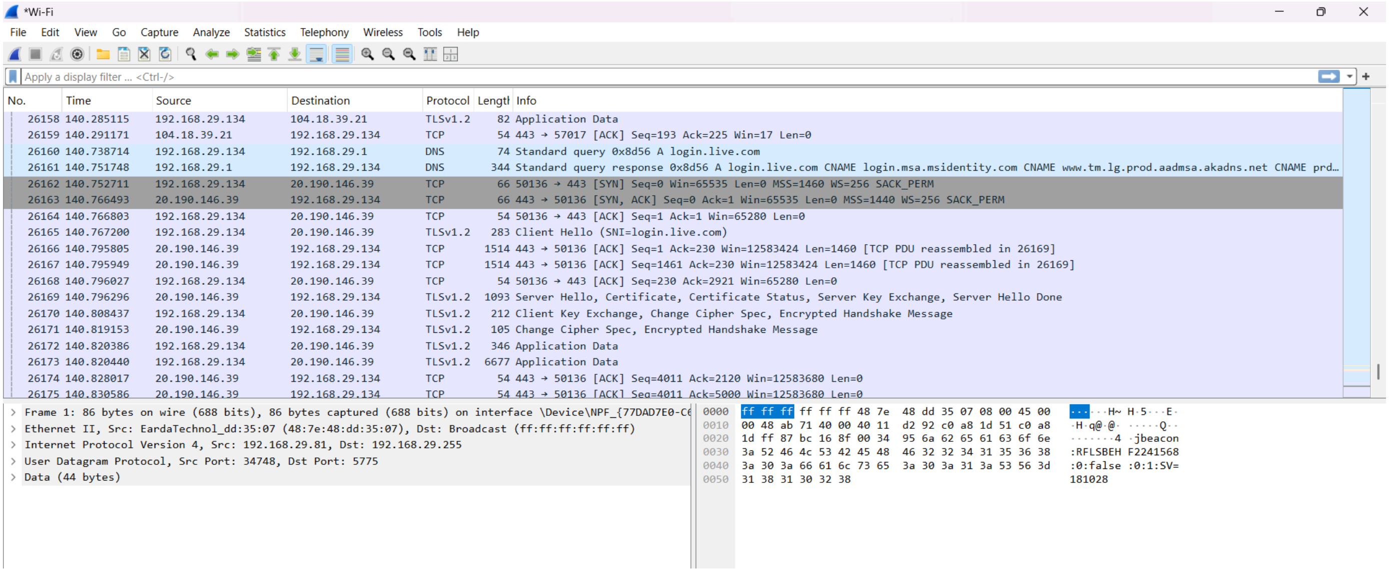
   ○ Disconnect from ProtonVPN.

   ○ Start a new Wireshark capture on the same interface.

   ○ Visit the same websites.

   ○ Stop after 1–2 minutes.

   ○ You'll notice some traffic is still HTTPS (encrypted), but DNS queries and certain connections may be visible in plaintext, revealing hostnames and IPs.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source          Destination     Protocol Lengtl Info
26158 140.285115 192.168.29.134  104.18.39.21    TLSv1.2    82 Application Data
26159 140.291171 104.18.39.21    192.168.29.134  TCP        54 443 → 57017 [ACK] Seq=193 Ack=225 Win=17 Len=0
26160 140.738714 192.168.29.134  192.168.29.1    DNS        74 Standard query 0x8d56 A login.live.com
26161 140.751748 192.168.29.1    192.168.29.134  DNS       344 Standard query response 0x8d56 A login.live.com CNAME login.msa.msidentity.com CNAME www.tm.lg.prod.aadmsa.akadns.net CNAME prd…
26162 140.752711 192.168.29.134  20.190.146.39   TCP        66 50136 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
26163 140.766493 20.190.146.39   192.168.29.134  TCP        66 443 → 50136 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
26164 140.766803 192.168.29.134  20.190.146.39   TCP        54 50136 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
26165 140.767200 192.168.29.134  20.190.146.39   TLSv1.2   283 Client Hello (SNI=login.live.com)
26166 140.795805 20.190.146.39   192.168.29.134  TCP      1514 443 → 50136 [ACK] Seq=1 Ack=230 Win=12583424 Len=1460 [TCP PDU reassembled in 26169]
26167 140.795949 20.190.146.39   192.168.29.134  TCP      1514 443 → 50136 [ACK] Seq=1461 Ack=230 Win=12583424 Len=1460 [TCP PDU reassembled in 26169]
26168 140.796027 192.168.29.134  20.190.146.39   TCP        54 50136 → 443 [ACK] Seq=230 Ack=2921 Win=65280 Len=0
26169 140.796296 20.190.146.39   192.168.29.134  TLSv1.2  1093 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
26170 140.808437 192.168.29.134  20.190.146.39   TLSv1.2   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
26171 140.819153 20.190.146.39   192.168.29.134  TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
26172 140.820386 192.168.29.134  20.190.146.39   TLSv1.2   346 Application Data
26173 140.820440 192.168.29.134  20.190.146.39   TLSv1.2  6677 Application Data
26174 140.828017 20.190.146.39   192.168.29.134  TCP        54 443 → 50136 [ACK] Seq=4011 Ack=2120 Win=12583680 Len=0
26175 140.830586 20.190.146.39   192.168.29.134  TCP        54 443 → 50136 [ACK] Seq=4011 Ack=5000 Win=12583680 Len=0
```

```
> Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{77DAD7E0-C6
> Ethernet II, Src: EardaTechnol_dd:35:07 (48:7e:48:dd:35:07), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.29.81, Dst: 192.168.29.255
> User Datagram Protocol, Src Port: 34748, Dst Port: 5775
> Data (44 bytes)
```

```
0000  ff ff ff ff ff ff 48 7e  48 dd 35 07 08 00 45 00   ······H~ H·5···E·
0010  00 48 ab 71 40 00 40 11  d2 92 c0 a8 1d 51 c0 a8   ·H·q@·@· ·····Q··
0020  1d ff 87 bc 16 8f 00 34  95 6a 62 65 61 63 6f 6e   ·······4 ·jbeacon
0030  3a 52 46 4c 53 42 45 48  46 32 32 34 31 35 36 38   :RFLSBEH F2241568
0040  3a 30 3a 66 61 6c 73 65  3a 30 3a 31 3a 53 56 3d   :0:false :0:1:SV=
0050  31 38 31 30 32 38                                  181028
```

4. **Interpret the Results**

   ○ With VPN ON - all traffic goes through the encrypted tunnel, so intercepted packets are unreadable.

   ○ Without VPN - some metadata (like DNS requests) and IP connections can be visible to anyone monitoring the network, even if the content is HTTPS.

VPN Concept Note for this step:

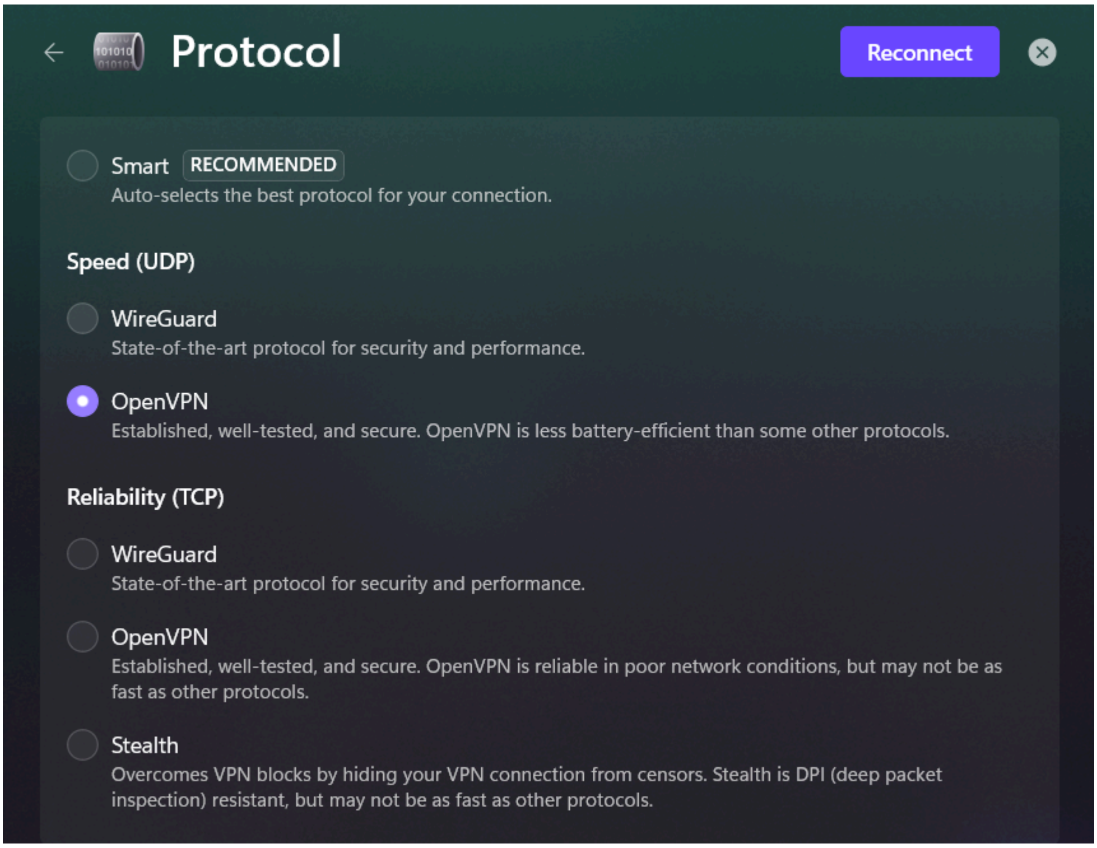
- VPNs enhance **network security** by encrypting **all** traffic between your device and the VPN server, hiding even metadata from local attackers (e.g., on public Wi-Fi).

Step 5 Compare WireGuard vs OpenVPN in ProtonVPN

We'll switch the VPN tunneling protocol, repeat the packet capture, and note the differences.

1. Switch Protocol in ProtonVPN

1. Disconnect from your current VPN connection.
2. In ProtonVPN, go to **Settings > Connection**.
3. Find **VPN Protocol** and change it from **WireGuard** to **OpenVPN (UDP)**.
4. Save/apply the change.



○ Smart RECOMMENDED
Auto-selects the best protocol for your connection.

Speed (UDP)

○ WireGuard
State-of-the-art protocol for security and performance.

● OpenVPN
Established, well-tested, and secure. OpenVPN is less battery-efficient than some other protocols.

Reliability (TCP)

○ WireGuard
State-of-the-art protocol for security and performance.

○ OpenVPN
Established, well-tested, and secure. OpenVPN is reliable in poor network conditions, but may not be as fast as other protocols.

○ Stealth
Overcomes VPN blocks by hiding your VPN connection from censors. Stealth is DPI (deep packet inspection) resistant, but may not be as fast as other protocols.

2. Connect Using OpenVPN

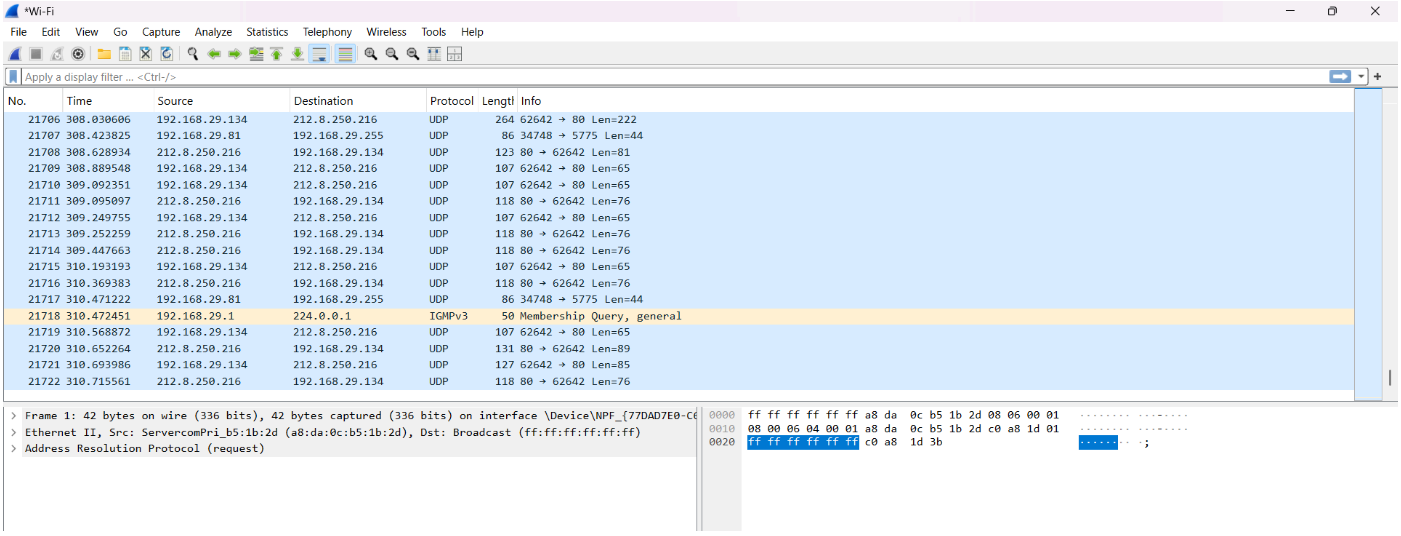
1. Reconnect to the same country (Netherlands free server) so location variables stay the same.
2. Confirm in the connection details that it shows **OpenVPN UDP**.

3. Capture Traffic with Wireshark

1. Open Wireshark and select your active network interface.
2. Start capturing packets.
3. Browse a couple of websites.

4. Stop the capture after 1–2 minutes.

5. Check the **Protocol** column; you should now see **OpenVPN** instead of WireGuard.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time        Source           Destination      Protocol Lengtl Info
 21706 308.030606  192.168.29.134   212.8.250.216    UDP       264 62642 → 80 Len=222
 21707 308.423825  192.168.29.81    192.168.29.255   UDP        86 34748 → 5775 Len=44
 21708 308.628934  212.8.250.216    192.168.29.134   UDP       123 80 → 62642 Len=81
 21709 308.889548  192.168.29.134   212.8.250.216    UDP       107 62642 → 80 Len=65
 21710 309.092351  192.168.29.134   212.8.250.216    UDP       107 62642 → 80 Len=65
 21711 309.095097  212.8.250.216    192.168.29.134   UDP       118 80 → 62642 Len=76
 21712 309.249755  192.168.29.134   212.8.250.216    UDP       107 62642 → 80 Len=65
 21713 309.252259  212.8.250.216    192.168.29.134   UDP       118 80 → 62642 Len=76
 21714 309.447663  212.8.250.216    192.168.29.134   UDP       118 80 → 62642 Len=76
 21715 310.193193  192.168.29.134   212.8.250.216    UDP       107 62642 → 80 Len=65
 21716 310.369383  212.8.250.216    192.168.29.134   UDP       118 80 → 62642 Len=76
 21717 310.471222  192.168.29.81    192.168.29.255   UDP        86 34748 → 5775 Len=44
 21718 310.472451  192.168.29.1     224.0.0.1        IGMPv3     50 Membership Query, general
 21719 310.568872  192.168.29.134   212.8.250.216    UDP       107 62642 → 80 Len=65
 21720 310.652264  212.8.250.216    192.168.29.134   UDP       131 80 → 62642 Len=89
 21721 310.693986  192.168.29.134   212.8.250.216    UDP       127 62642 → 80 Len=85
 21722 310.715561  212.8.250.216    192.168.29.134   UDP       118 80 → 62642 Len=76
```

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{77DAD7E0-C6
> Ethernet II, Src: ServercomPri_b5:1b:2d (a8:da:0c:b5:1b:2d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff a8 da  0c b5 1b 2d 08 06 00 01   ........ ...-....
0010  08 00 06 04 00 01 a8 da  0c b5 1b 2d c0 a8 1d 01   ........ ...-....
0020  ff ff ff ff ff ff c0 a8  1d 3b                     ........ .;
```

4. Compare Findings

- **WireGuard:** Faster, uses UDP only, modern cryptography (ChaCha20), small codebase.
- **OpenVPN:** Slower, but very mature and highly configurable, uses AES-256 encryption.
- Both encrypt traffic and hide DNS, but the packet structure differs in Wireshark.

Feature	WireGuard	OpenVPN UDP
Speed	High	Moderate
Encryption	ChaCha20	AES-256
Code size	Small	Large
Visibility in Wireshark	Protocol shows as WireGuard	Protocol shows as OpenVPN