Create a Digital Ocean account
Create a Droplet in Digital Ocean

1. Use this link to [DigitalOcean.com] (https://m.do.co/c/d33d59113ab6) to sign up with your school email and Agent Miller’s credit card
2. Choose the lowest price tier - $6 per month
3. Create an Ubuntu droplet
4. Select all the basic options
5. Choose password instead of ssh key
6. Name the project -
7. Droplet IP

Terminal:

1. **Connect to the droplet you just made:**

    1. Cmd: ssh root@165.232.143.161

    2. Say yes to continue connecting and input the password you made during setup

2. **Docker install**: [https://thematrix.dev/install-docker-and-docker-compose-on-ubuntu-20-04/] (https://thematrix.dev/install-docker-and-docker-compose-on-ubuntu-20-04/)

    1. **Install necessary tools**:

        1. Cmd: sudo apt install apt-transport-https ca-certificates curl software-properties-common -y

    2. **Add Docker Key**

        1. Cmd: curl -fsSL [https://download.docker.com/linux/ubuntu/gpg] (https://download.docker.com/linux/ubuntu/gpg) | sudo apt-key add -

    3. **Add docker repo**

        1. 32bit / 64bit OS

            1. Cmd: sudo add-apt-repository \"deb [arch=amd64] [https://download.docker.com/linux/ubuntu] (https://download.docker.com/linux/ubuntu) \$(lsb_release -cs) \stable"

        2. **Switch to repo**

            1. Cmd: apt-cache policy docker-ce

    4. **Install Docker**

        1. Cmd: sudo apt install docker-ce -y

        2. **Run without root:**

            1. Cmd: sudo usermod -aG docker ${USER}

    5. **Install Docker-Compose**

        1. Cmd: sudo curl -L "https://github.com/docker/compose/releases/download/1.27.4/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose

        2. Permissions

            1. Cmd: sudo chmod +x /usr/local/bin/docker-compose

    6. **Docker check**

        1. sudo docker run hello-world

        2. docker compose version

3. **WireGuard setup:**

    1. Make directories for wireguard config and a yml file for compose

        1. Cmd:

            ```
            mkdir -p ~/wireguard/
            mkdir -p ~/wireguard/config/
            nano ~/wireguard/docker-compose.yml
            ```

        2. Paste config below into the nano:

            1.

                ```
                version: '3.8'
                services:
                  wireguard:
                ```

```
container_name: wireguard

image: linuxserver/wireguard

environment:

  - PUID=1000

  - PGID=1000

  - TZ=Asia/Hong_Kong

  - SERVERURL=1.2.3.4

  - SERVERPORT=51820

  - PEERS=pc1,pc2,phone1

  - PEERDNS=auto

  - INTERNAL_SUBNET=10.0.0.0

ports:

  - 51820:51820/udp

volumes:

  - type: bind

    source: ./config/

    target: /config/

  - type: bind

    source: /lib/modules

    target: /lib/modules

restart: always

cap_add:
```

```
                                        - NET_ADMIN

                                        - SYS_MODULE

                                       sysctls:

                                        - net.ipv4.conf.all.src_valid_mark=1
```

- TZ needs to be changed for your time zone, I am cst so i am in america/chicago which is CST6CDT
- SERVERURL is the address of your droplet server, the one you used to in the ssh root@ command

4. **Starting Wireguard**

   1. Cmd: cd ~/wireguard/

   2. Cmd: docker-compose up -d

5. **Check logs to get the QR code**:

docker logs wireguard

Test Your VPN

Mobile Device

1. Open the Wireguard app and scan the QR code from the logs.
2. **Before connecting**:
3. Visit [IPLeak.net](https://ipleak.net/) and screenshot your local IP.
4. **After connecting**:
5. Turn on the Wireguard VPN and revisit IPLeak.net.
6. Screenshot the VPN IP to confirm it is active.

Laptop

1. Install the Wireguard app for your laptop: https://www.wireguard.com/install/

2. Launch the program and select the add tunnel dropdown on the left hand side of the screen, then click add empty tunnel.

3. Upon creation a dialog box will pop up, with the text

   1. [Interface]

   2. PrivateKey= (whatever your private key is)

5. Next go back to terminal and find your peer.conf files

    1. cd ~/wireguard/

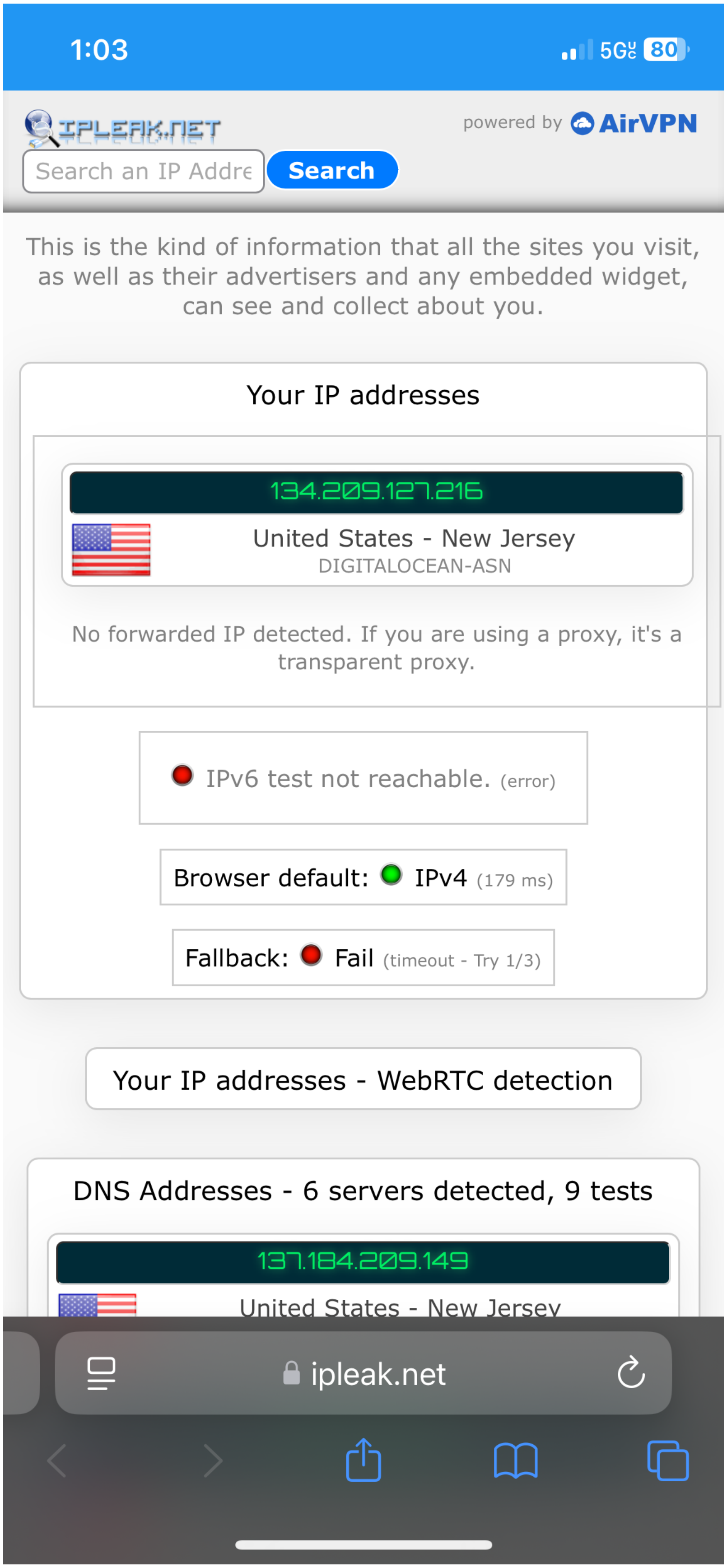
    2. cd config

    3. cd peer_pc1 (that was one of the peer names set, if you named it differently than your command will be cd (yourpeername))

    4. cat peer_pc1.conf (cat your peer file)

6. After using cat on your peer.conf file copy all the contents over to the dialog box fireguard produced when adding an empty terminal and ensure that it replaces what came with the dialog box.

7. Give the tunnel a name and click save, afterwards hit the activate button and your vpn should work.



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

134.209.127.216
United States - New Jersey
DIGITALOCEAN-ASN

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

● IPv6 test not reachable. (error)

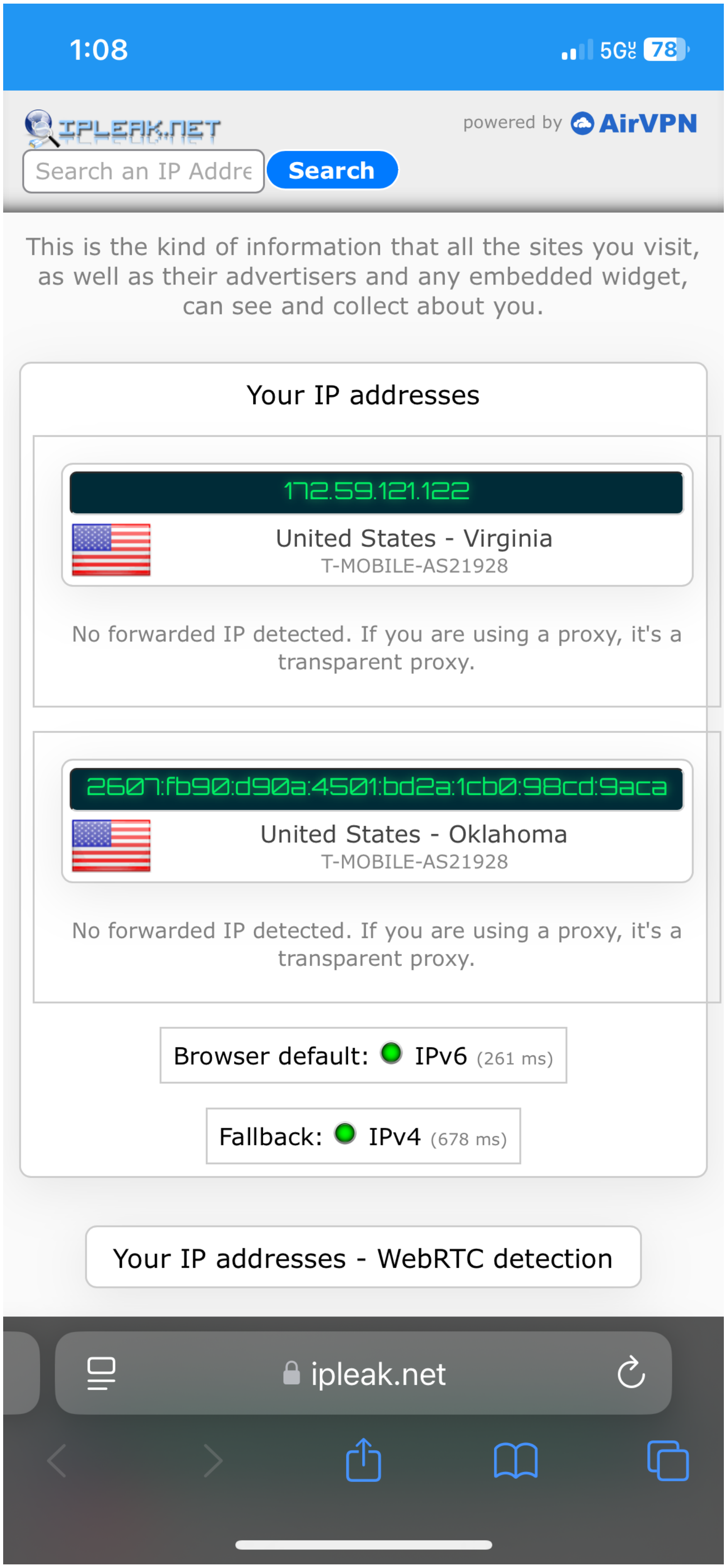
Browser default: ● IPv4 (179 ms)

Fallback: ● Fail (timeout - Try 1/3)

Your IP addresses - WebRTC detection

DNS Addresses - 6 servers detected, 9 tests

137.184.209.149
United States - New Jersey



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

172.59.121.122

United States - Virginia
T-MOBILE-AS21928

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

2607:fb90:d90a:4501:bd2a:1cb0:98cd:9aca

United States - Oklahoma
T-MOBILE-AS21928

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

Browser default: ● IPv6 (261 ms)

Fallback: ● IPv4 (678 ms)

Your IP addresses - WebRTC detection