Make sure your tor service is running on boot, on Arch Linux, to start the tor service and run it, run the following commands in the terminal:

- sudo systemctl enable tor
- sudo systemctl start tor

Check if it is running in linux with the following command:

- systemctl status tor

In your tor configuration file, which on linux, can be found in **\etc\tor\torrc**, add the following lines:

MaxCircuitDirtiness 60
NewCircuitPeriod 30

MaxCircuitDirtiness enables how often tor will change the IP address. In this example I have set it to 30 seconds, but it can be set as low as 10 seconds. New circuit period refers to how often to change the circuit, which contains a list of randomly selected IP addresses. Unfortunately, from many test runs, I noticed that some of these IP addresses have already been banned by plugshare. In this example, it has been set to change the circuit every 30 seconds.
More options that I have not explored can be found here.
In the "CTScraper_ProxyWorking.js" file, some new options have been added, specifically the following:

- minConcurrency: 1
- maxConcurrency: 2
- maxRequestsPerMinute: 10

Which are the default values. I recommend keeping the first two the same, maybe the second one can go to 3, **but no higher**. The second, I recommend going **no more than 20**, as too many requests can overwhelm the website. I noticed that some of the tor IP addresses have a 403 error code going to Plugshare, so there is a strong potential for more IP addresses to get **permanently banned**. If you increases these settings from my suggestions **STOP** around 6000 observations for around 2 hours.
Test runs always finish around 1 hour so I believe this suitable for long term scraping.