

Before turning on VPN:

The screenshot shows the iPLEAK.NET website interface. At the top, the status bar displays the time 6:42, signal strength, Wi-Fi, and battery at 42%. The website header includes the iPLEAK.NET logo, a search bar with the text "Search an IP Address", and a "Search" button. Below the header, a message states: "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."

The main section is titled "Your IP addresses". It displays the IP address 129.244.19.53 in green text on a dark background. Below the IP address is a small American flag icon and the text "United States - Oklahoma" and "UTULSA-AS". A note below this says: "No forwarded IP detected. If you are using a proxy, it's a transparent proxy."

Below the IP address section, there are three status boxes:

- IPv6 test not reachable. (error) - indicated by a red dot.
- Browser default: IPv4 (514 ms) - indicated by a green dot.
- Fallback: Fail (timeout - Try 2/3) - indicated by a red dot.

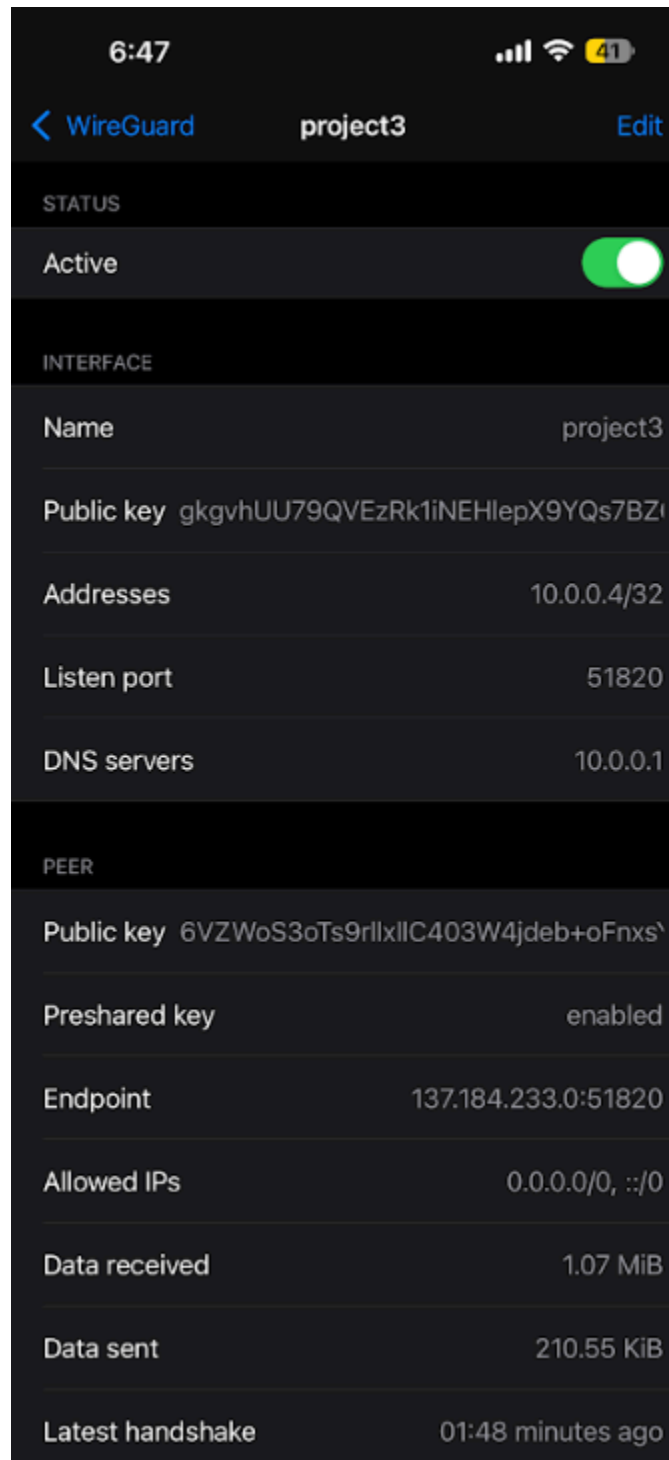
The next section is titled "Your IP addresses - WebRTC detection".

Below that is a section titled "DNS Addresses - 6 servers detected, 25 tests". It contains the text: "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](#)".

The next section is titled "Torrent Address detection". It contains a button labeled "Activate".

At the bottom of the page, there is a footer that says "Not Secure — ipleak.net".

Activating VPN Tunnel:



After Activating VPN:

