

Forum:[Hack Forums](#)

Thread: [How to Deauth 5GHz Networks using an ESP32-C5 & Bruce Firmware \(Step-by-Step Guide\)](#)

Wake - September 2, 2026, 11:17 am

? loading encrypted image...

How to Deauth 5GHz Networks using an ESP32-C5 & Bruce Firmware
(Step-by-Step Guide)

? loading encrypted image...

Written by [Wake](#)

? loading encrypted image...

About this thread

This thread assumes you already have Bruce flashed onto your ESP32-C5. If you haven't flashed your board yet or aren't sure which hardware works, check out my previous guide:

<https://hackforums.net/showthread.php?tid=6330964>

For more in-depth guidance feel free to convo me.

Disclaimer

This thread is for informational and educational purposes only. I will not be responsible for any action performed by any reader.

Introduction

In this tutorial, I will walk you through step-by-step how to deauth a 5GHz network using Bruce firmware on an ESP32-C5, identifying 5GHz networks, understanding 5GHz vs 2.4GHz networks and why some 5GHz networks won't be affected by this type of attack.

What will I need for this?

[+] Chrome browser (Any browser with web serial support)

[+] ESP32-C5 (Waveshare ESP32-C5-WIFI6-KIT-NXRX)

[+] USB C Cable (data cable, not just charging)

? loading encrypted image...

2.4GHz vs 5GHz Wi-Fi

Modern wireless routers broadcast network traffic over two distinct radio frequency bands: 2.4GHz and 5GHz.

2.4GHz Band: Broadcasts on lower frequencies giving it longer range and the ability to pass through solid objects and walls easily. It can get heavily crowded with bluetooth devices, smart home devices and surrounding routers. 2.4GHz band broadcasts on channels 1 to 13/14. Standard ESP32 boards only operate on this single band.

5GHz Band: Broadcasts on higher frequencies offering much faster speeds with less interference, its higher frequency means it won't penetrate walls as well and is shorter in range. 5GHz band broadcasts on channels 36 to 165, we will use this channel information to later identify what network is our 5GHz network.

What is an ESP32-C5?

The ESP32-C5 is an SoC (System on chip) designed by Espressif Systems released April/May 2025. It is part of the popular ESP32 family of microcontrollers, but it has one major upgrade over nearly all the previous models. The C5 is the first chip that supports dual-band 2.4GHz and 5GHz wireless, allowing firmware like Bruce and Hale Hound to interact with modern 5GHz networks, something older ESP32 boards simply can't do.

What is Bruce?

Bruce is an open-source firmware built for ESP32 microcontrollers. Designed for security research and pentesting, it packages a wide range of tools into a single interface. Unlike firmware that requires a physical screen Bruce includes a web navigator, that's what we will be using later in this guide. If you would like more information about Bruce or the features I will leave the [Bruce Wiki here](#).

Devices running Bruce, Hale Hound (and similar firmware) are often nicknamed "budget Flipper Zero" alternatives due to their portability and wide range of features.

? loading encrypted image...

How do I do this?

[+] First step is with our USB C cable plugging our ESP32-C5 board into our machine.

[+] Now we need to head over to [the bruce web navigator](#).

[+] Once at the web navigator connect to your board through the web serial.

[+] Now we have our board connected at the bottom we need to select "navigator".

[+] Once you're on the navigator select WiFi, then WiFi Atks.

[+] Now select target atks and Bruce will scan for AP's, we know from before that 5GHz networks broadcast on a higher frequency, frequencies between 36 to 165. Once the scan is complete look for your SSID in the list and check its channel number.

[+] Now we have located our 5GHz network and selected it we have a new list of options.

[+] Scroll down to deauth and select it, it will now prepare and deauth your 5GHz network.

[+] Spoiler [\(Click to View\)](#)? loading encrypted image...

? loading encrypted image...

Why won't this work on every device?

During your testing you may find that certain 5GHz networks or devices refuse to disconnect when targeted. Some clients may ignore or resist forged management frames due to security features, driver behavior, or implementation differences. Results are highly device dependent.

If your target stays connected it doesn't mean your ESP32-C5 or Bruce firmware failed it just means the network or client device is properly secured against deauth attacks.

Finished Result

If everything was done correctly, you now have successfully deauthed a 5GHz network using an ESP32-C5 running Bruce firmware.

If you run into any issues, feel free to reply and I'll help out.

[Thank you for taking the time to read this thread. If you enjoyed this please check out the rest of my tutorials and write-ups](#)

luddite - September 3, 2026, 10:30 am

the fragging option in MDK4 will get handshakes as well.

but its global and your own routers may need a reset after a while.

Wake - September 3, 2026, 3:14 pm

(Sep 3, 2026 10:30 AM)luddite Wrote: [\[CITE\]](#) the fragging option in MDK4 will get handshakes as well.

but its global and your own routers may need a reset after a while.

Appreciate the read and the reply, MDK4 is a great CLI tool, but if you are looking for something a little more portable I have a tutorial on how to capture handshakes with a CYD and Hale Hound.

<https://hackforums.net/showthread.php?tid=6323296>