# Flipper Zero Demonstrations

Ethan Kanyid

What is the Flipper Zero?

- The Flipper Zero is a pocket-sized, consumer-friendly gadget that can interact with many of the signals all around us, making it useful for hobbyists and security researchers.

- Capabilities include:
  - Sub-1 GHz Radio
  - RFID / NFC (Low & High Frequency)
  - Infrared (IR)
  - iButton / 1-Wire
  - BadUSB
  - App Store & Extensibility

- It also has GPIO pins and a USB C port for added extensibility
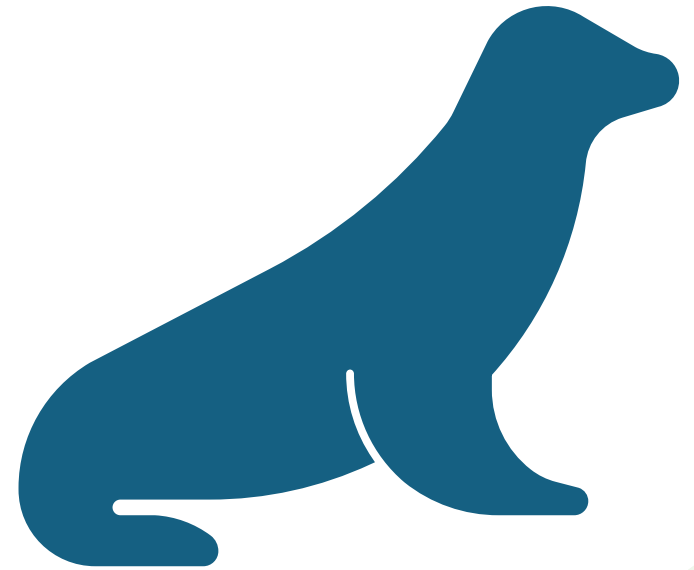
Technicalities

- A strong understanding of wireless signals is necessary to use the Flipper Zero to its fullest capabilities.

- As well, experience with hardware and firmware is important to be able to unlock the Flipper Zero for even more potential.

- However, the UI is very simple, and it is easy to interact with

- Otherwise, the Flipper Zero is just a toy.
  - It can download some games
  - Mindless experimenting
  - Expensive dust collector

Progress

- Flipper Zero was flashed with the Unleashed custom firmware using the qFlipper app on macOS.
- Additional apps (BLE Spam, SubGHz remote, Wi-Fi marauder) were installed via the Flipper app on iOS.
- A Wi-Fi ESP32 dev board received custom firmware via macOS and an online flasher; devices were then connected and demonstrations performed.
  - NFC, SubGHz, Infrared, Bluetooth, Wi-Fi

Next Steps

Plan to measure the effects of the demonstrations using quantifiable metrics to assess Flipper Zero's usability.
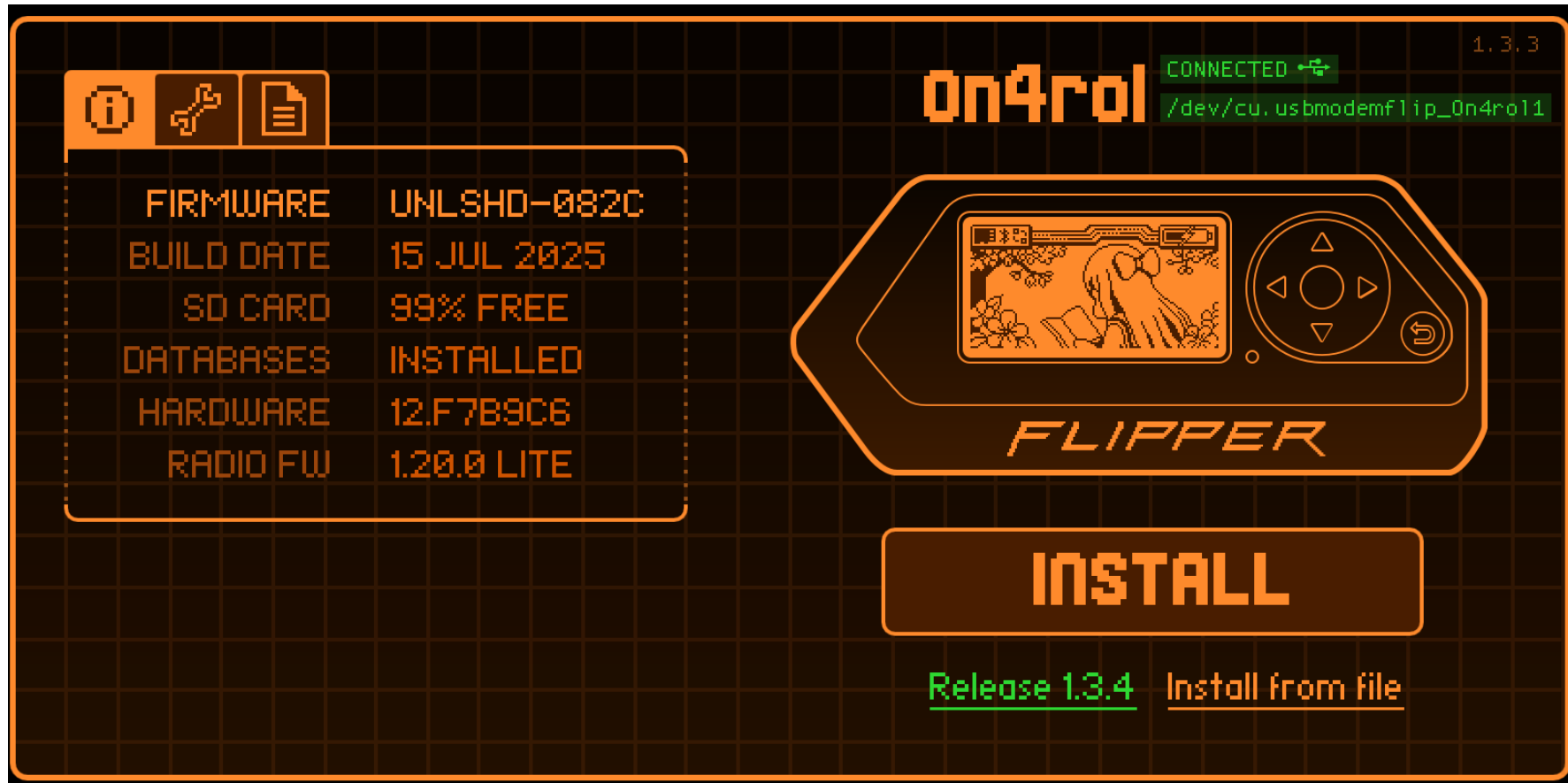
Document the entire process thoroughly to provide reproducible records.

Verify and validate each step to confirm legitimacy and accuracy of results.

Questions?

Demonstration