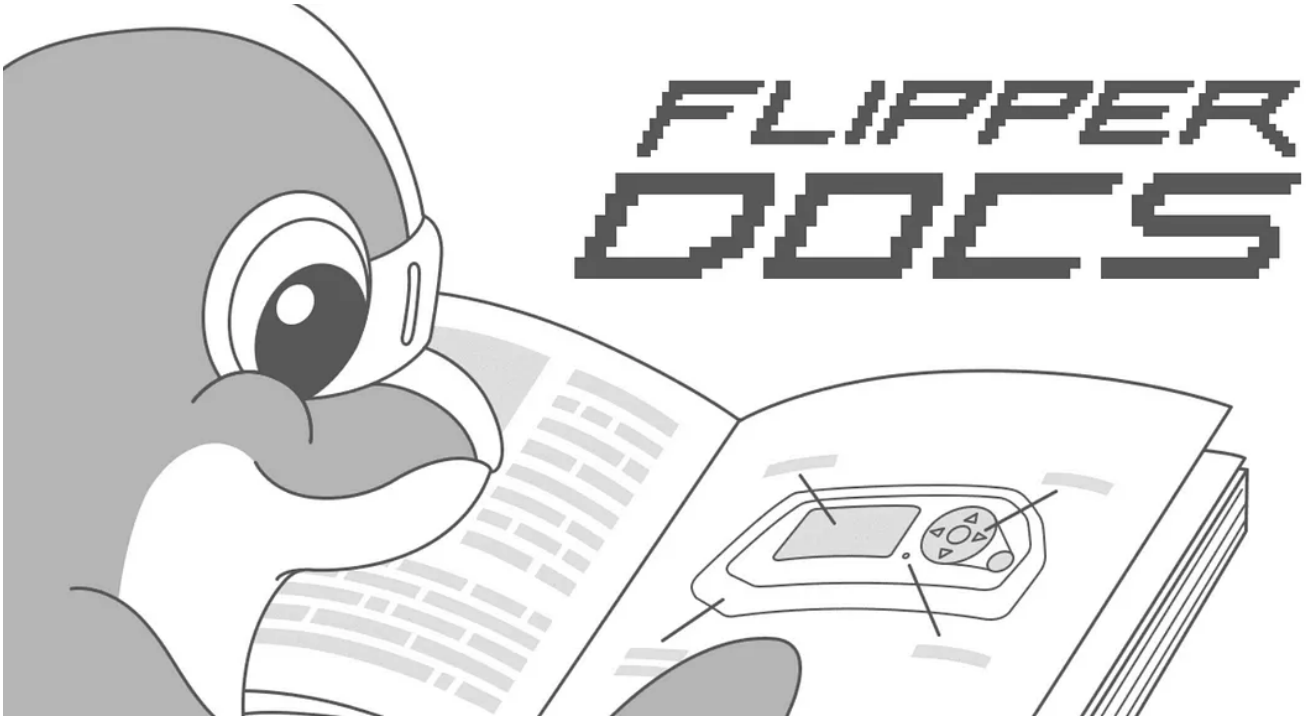
# The Ultimate Guide / CheatSheet to Flipper Zero

Ilias Mavropoulos · Follow

Published in InfoSec Write-ups · 19 min read · 5 days ago






## Table of Contents

## Section 0: Introduction

### 0.1 What Is the Flipper Zero?

Flipper Zero is a small, handheld device that combines the features of various hardware tools into one pocket-sized gadget. It's built primarily for interacting with digital and radio protocols, physical access systems, and various wireless devices. With its open-source nature and community-driven development, Flipper Zero stands out as a tool that evolves continuously, adapting to the latest trends and needs in the cybersecurity landscape. Flipper Zero is primarily designed for penetration testers, security researchers, and IT professionals, but its intuitive design makes it accessible even for hobbyists and tech enthusiasts.

### 0.2 Unique Features of Flipper Zero

1. **Multi-Protocol Support:** Flipper Zero's most striking feature is its ability to handle a wide array of protocols such as RFID, NFC, Infrared, Bluetooth, and more. This makes it a Swiss Army knife for wireless communication and hacking.
2. **User-Friendly Interface and Gamified UX:** Despite its advanced capabilities, Flipper Zero boasts an intuitive user interface with a simple navigation button and a small LCD screen, making it approachable for users of all skill levels.

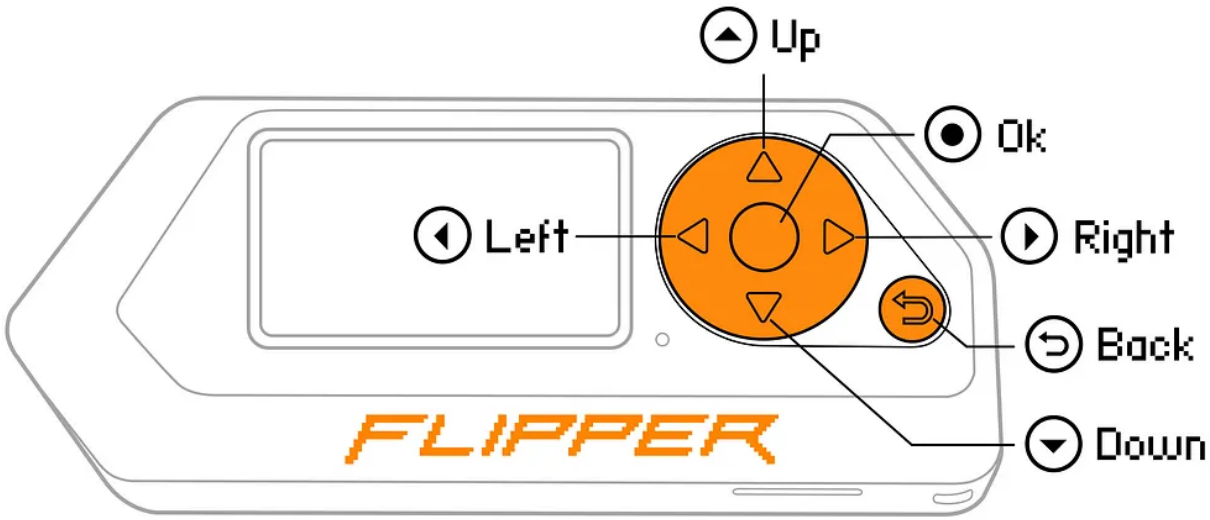
3. **Built-In Radio Modules:** The device is equipped with a variety of radio modules that allow it to interact with different wireless systems, making it perfect for real-world applications in penetration testing and red teaming.
4. **Customization and Modding:** Being open-source, Flipper Zero can be customized extensively. Users can write their own scripts, develop plugins, or even modify additional compatible hardware to suit specific needs.
5. **Portability and Durability:** Designed to fit in your pocket, Flipper Zero is the epitome of portability. Its robust build quality ensures that it can withstand the rigors of fieldwork.
6. **Community-Driven Development:** The Flipper Zero community plays a vital role in its evolution, contributing to its firmware, developing new features, and providing comprehensive support to users.
7. **Battery Life:** With its long-lasting battery, Flipper Zero is designed for extended use, making it a reliable tool for on-the-go operations.
8. **Legal Compliance and Ethical Use:** The creators of Flipper Zero emphasize its use within the bounds of law and ethics, making it a tool for learning and responsible security testing.

## Section 1: Unveiling Flipper Zero

### 1.1 Description of the device controls

https://docs.flipper.net/basics/control

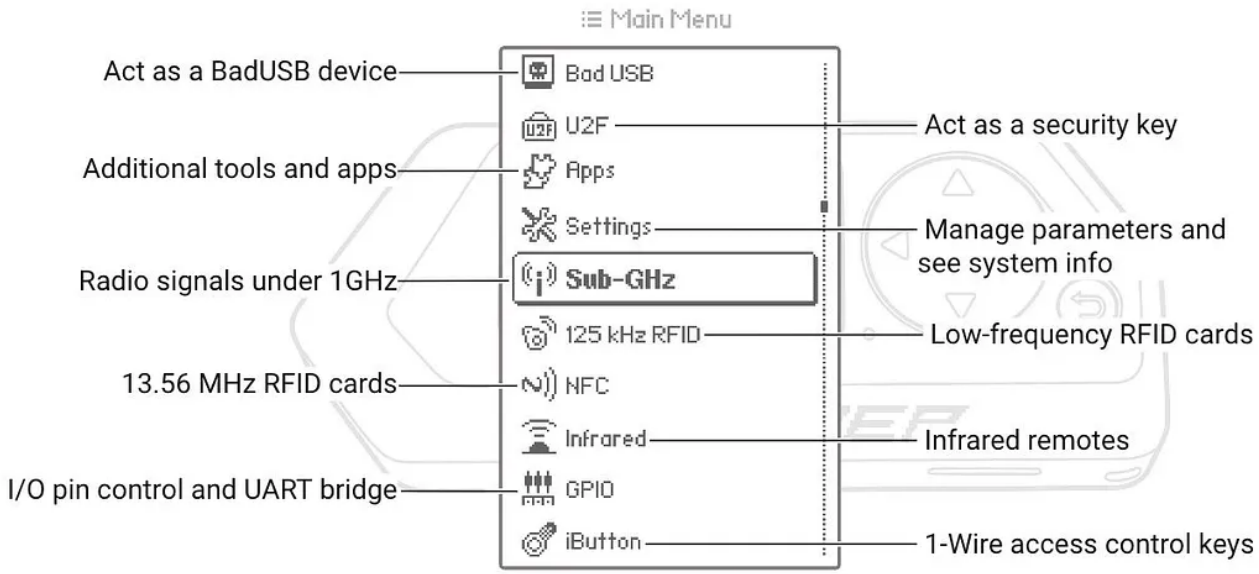
### Input Controls




You can control your Flipper Zero using a directional pad consisting of four buttons (**UP**, **DOWN**, **LEFT**, and **RIGHT**), the **OK** button located in the center of the pad, and the **BACK** button positioned beside the pad.

## Main Menu

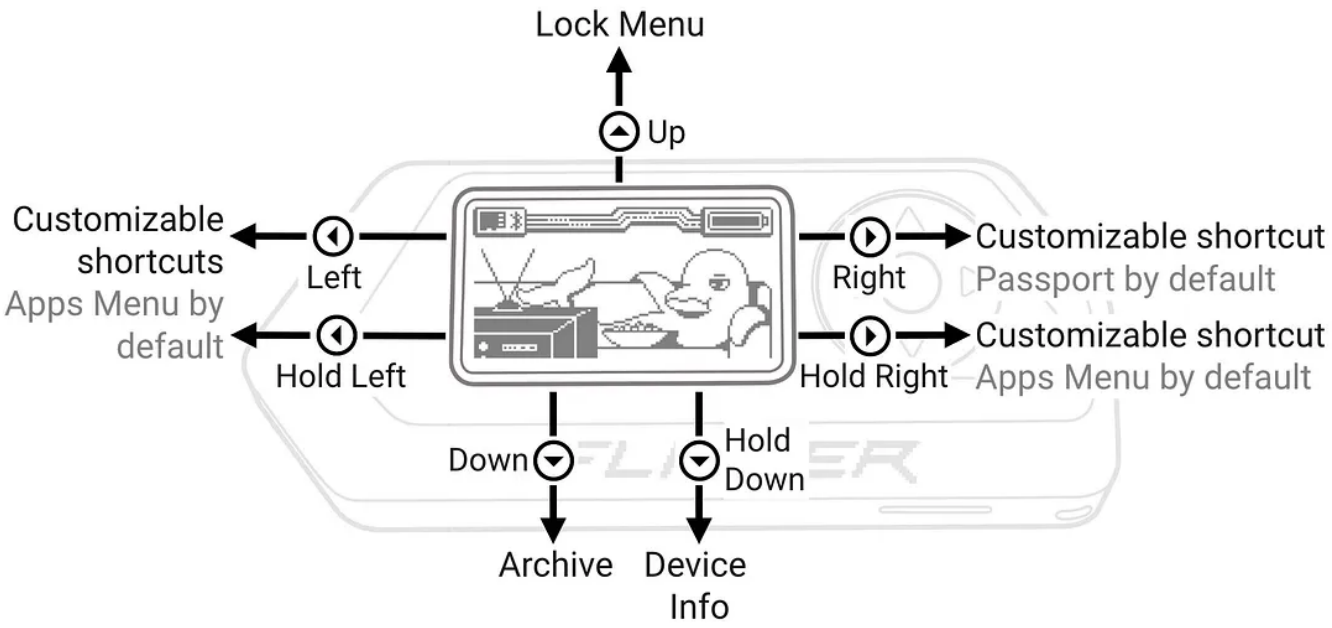
The Main Menu provides access to various features, settings, and apps. To access the Main Menu, press the **OK** button while on the Desktop.



Access apps in the Main Menu

## Desktop

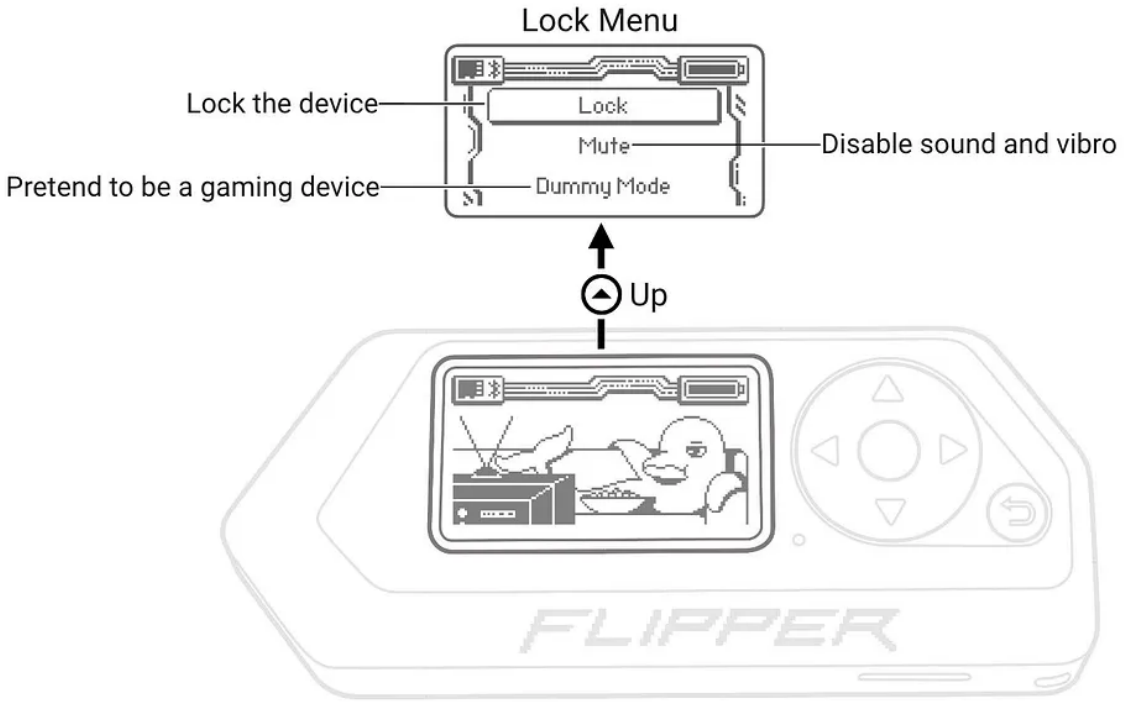
The Desktop is your digital pet's home. It's the place to see what your dolphin pet is doing and how it's feeling. You can view different indicators at the top of the desktop, including battery level, charging status, Bluetooth connectivity, microSD card status, and others.




Your digital pet lives on the Desktop

## Lock Menu

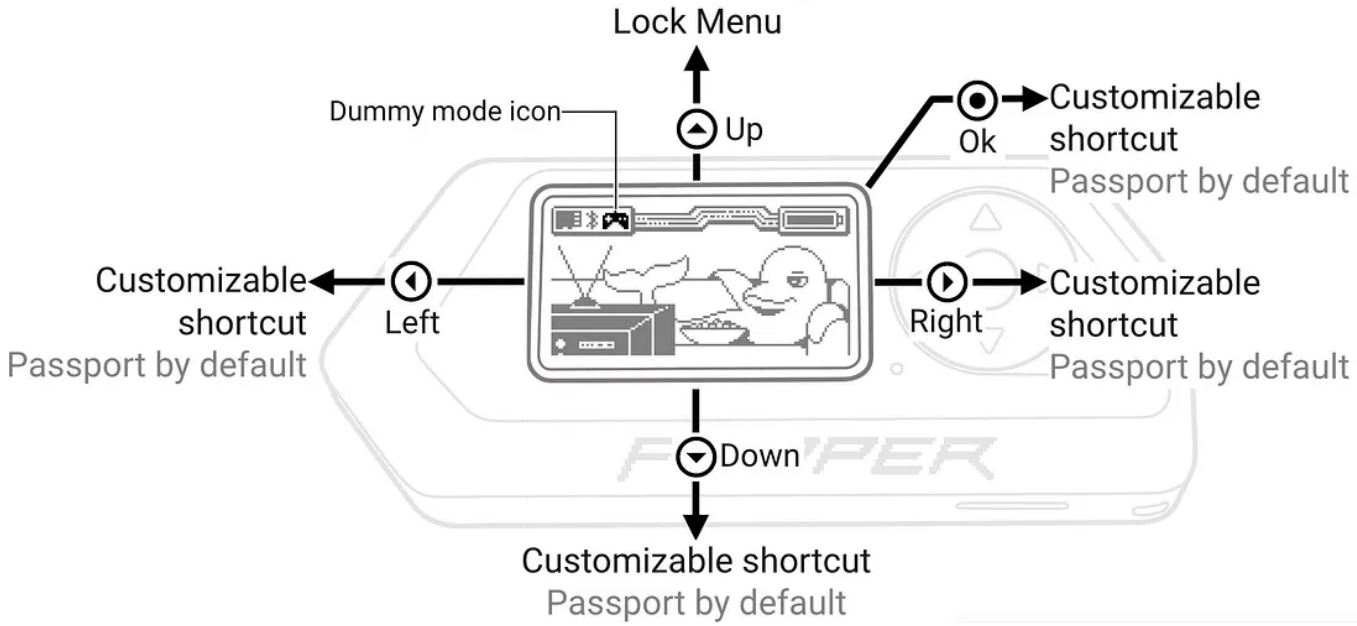
In the Lock Menu, you can lock your Flipper Zero with and without a PIN code, activate Dummy Mode, and mute the device. To enter the Lock Menu, press **UP** while on the Desktop.




View all options by pressing the UP button

## Dummy mode

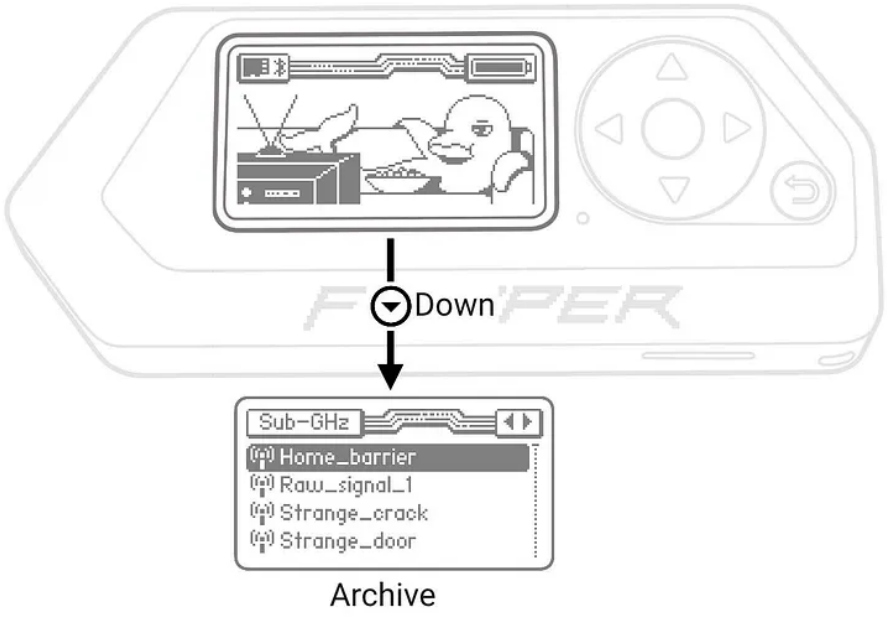
In this mode, Flipper Zero disables most of its functions. You can customize the controls by assigning quick-access apps of your choice to the **LEFT**, **RIGHT**, **DOWN**, and **OK** buttons.




In Dummy mode, your Flipper Zero turns into a gaming device

## Archive

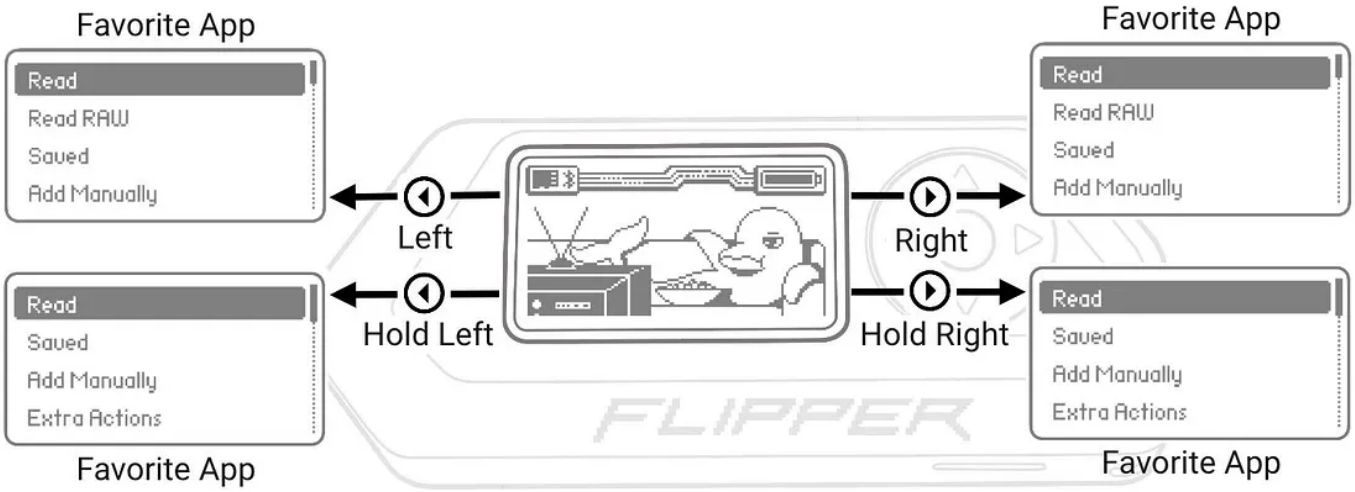
The Archive app lets you quickly access and manage saved tags, keys, remotes, payloads, and other apps.




Easily access your tags, keys, and remotes from the Desktop

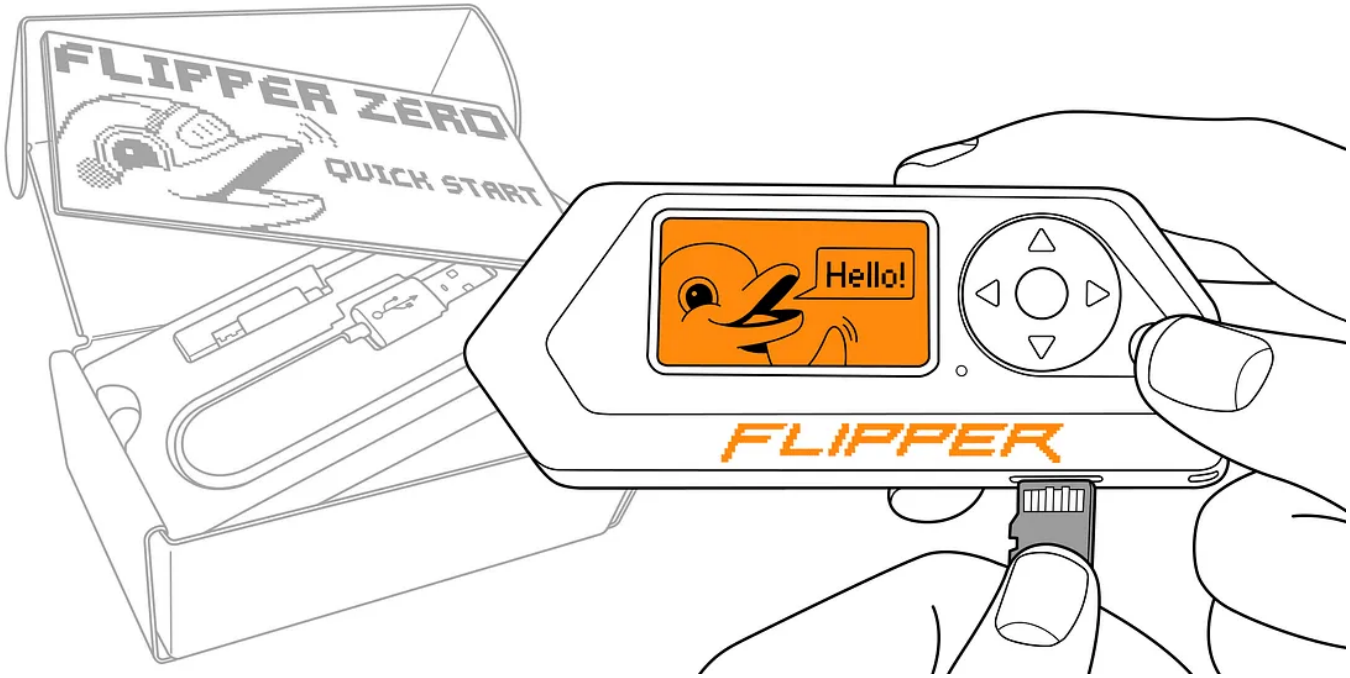
## Favorite Apps

The Favorite App feature allows you to set up to 4 apps for quick access directly from the Desktop. After that, you will not need to look for them in the Main Menu whenever you want to run them.




Access your favorite apps by pressing the LEFT and RIGHT buttons while on the Desktop

## 1.2 Initial Setup and first use.




### Initial Setup

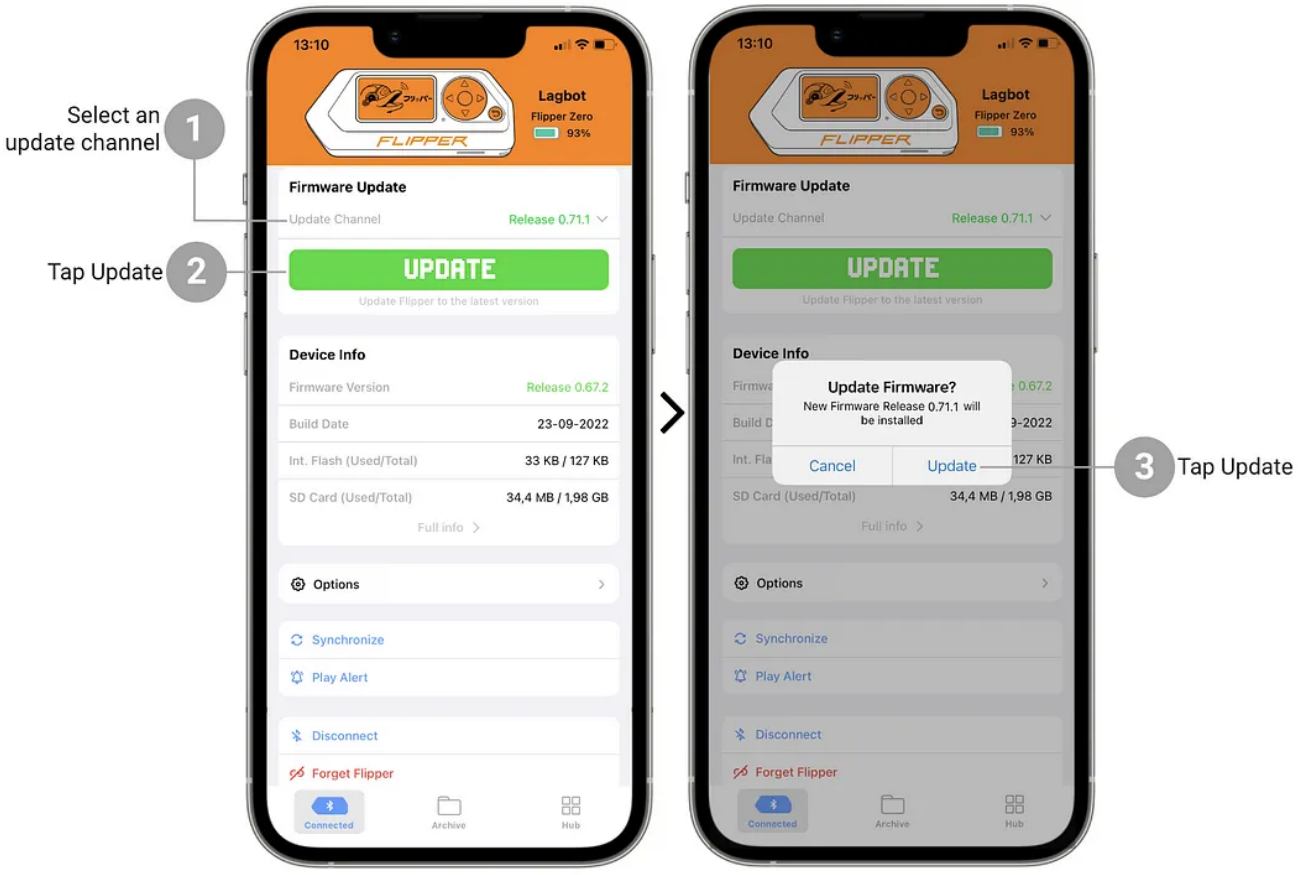
Flipper Zero does not come with a microSD card and it also cannot operate without one. So, you'll need to purchase one seperately.

> ***Note: Use a high-quality microSD card.***
> *It is important to use high-quality, branded microSD cards such as SanDisk, Kingston, Samsung, or others to ensure the proper performance of your Flipper Zero. Using low-quality microSD cards may not only result in poor performance but can also brick or even damage your device.*

## Initial Firmware Update

Before getting to know more your device more in-depth and discover your exact needs so you can may choose a custom firmware later, you may need to proceed with a stock firmware update before starting to play with the tool.

For a quick start I would recommend connecting Flipper Zero with your mobile device via Bluetooth and Update it via the Flipper Mobile App https://docs.flipper.net/mobile-app




You can update your Flipper Zero via the Flipper Mobile App

### What to do if your Flipper Zero Freezes

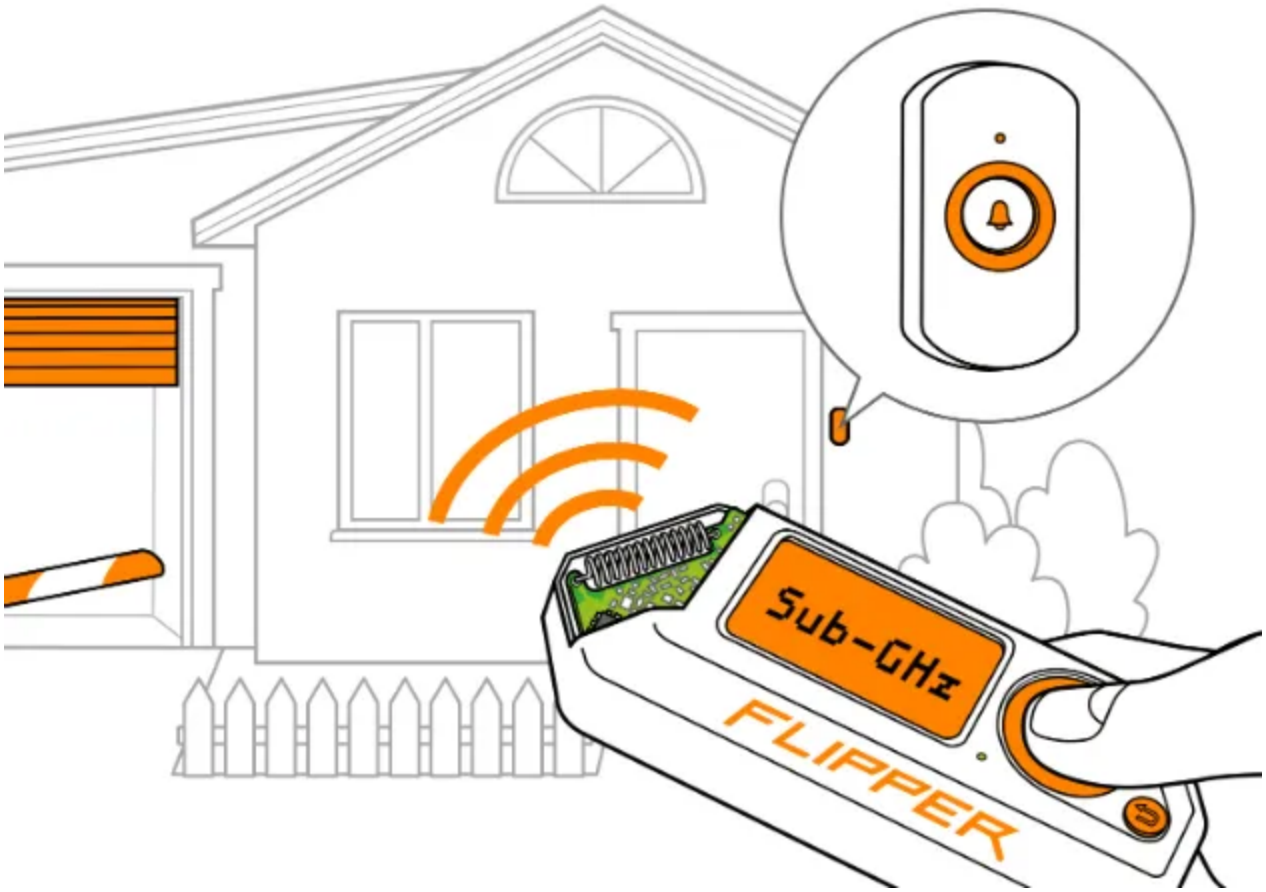
If your Flipper Zero freezes and fails to respond to button presses, reboot the device by pressing and holding the LEFT and BACK buttons for 5 seconds.


## Section 2: Basic Functionality and Maintenance

### 2.1 Exploring Basic Functions

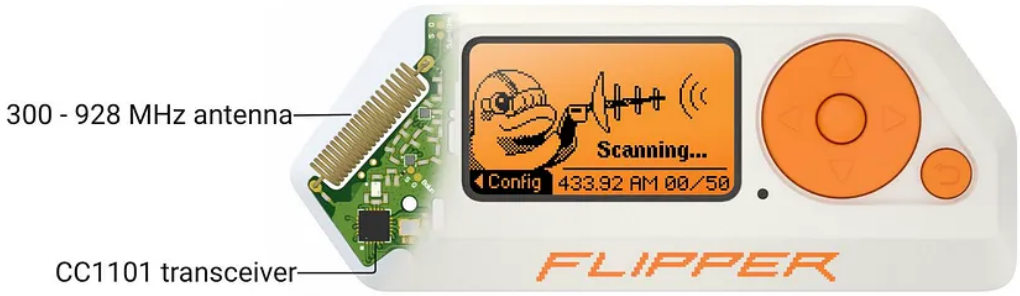
### Sub-GHz

https://docs.flipper.net/sub-ghz




Sub-GHz

The built-in module of Flipper Zero allows it to transmit and receive **radio frequencies between 300 and 928 MHz.** This capability enables it to read, store, and replicate remote controls. Such functionality is **crucial for interacting with various devices like gates, barriers, radio-controlled locks, remote switches, wireless doorbells, and smart lighting systems.** By using Flipper Zero, you can assess the robustness of your security systems, gaining insights into potential vulnerabilities.




Sub-GHz hardware

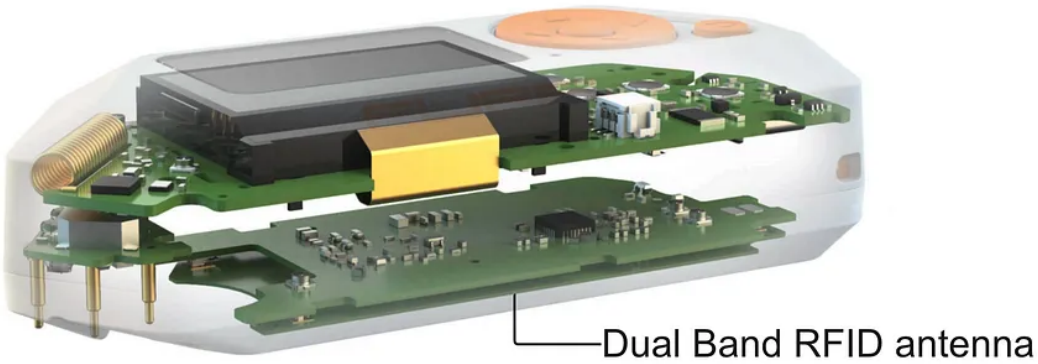
> *Flipper Zero has a built-in sub-1 GHz module based on a CC1101 transceiver and a radio antenna (the maximum range is 50 meters). Both the CC1101 chip and the antenna are designed to operate at frequencies in the 300–348 MHz, 387–464 MHz, and 779–928 MHz bands.*

### 125 kHz RFID

https://docs.flipper.net/rfid

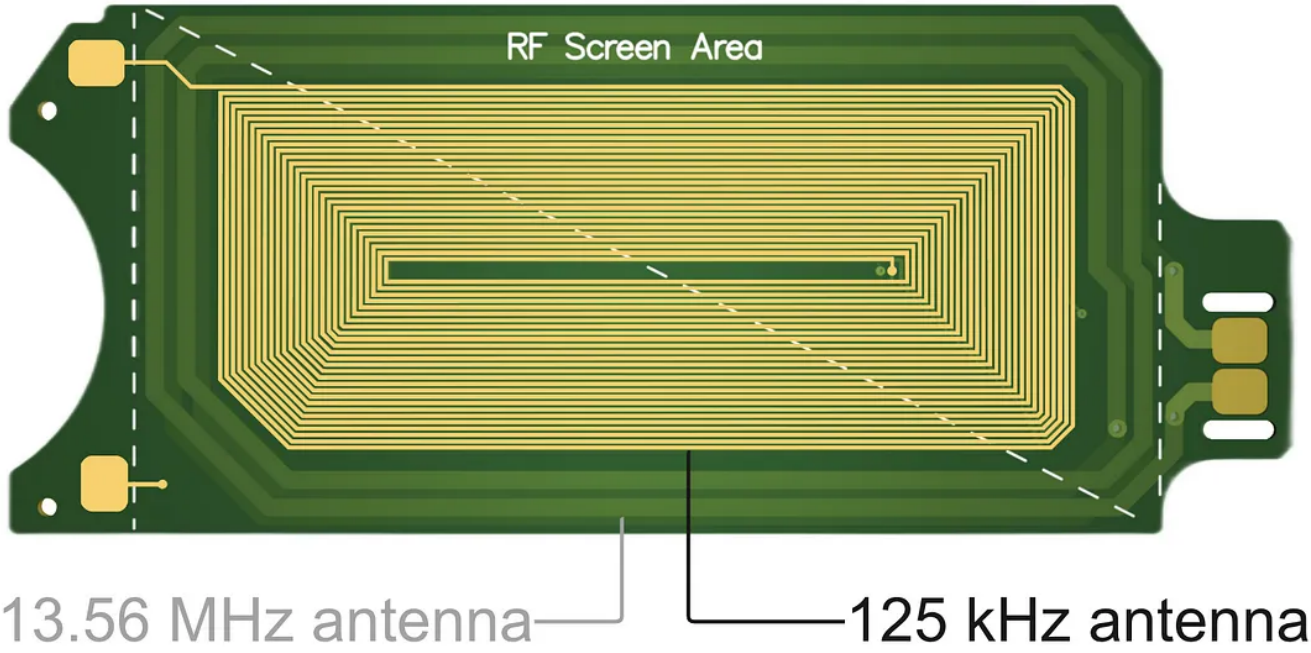
Flipper Zero is equipped with support for low-frequency (LF) radio frequency identification (RFID) technology, commonly **utilized in systems for access control, animal identification, and supply chain management.** LF RFID technology, which is generally found in items like plastic cards, key fobs, tags, wristbands, and animal microchips, **typically offers lower security levels compared to NFC cards.** The device includes a LF RFID module, enabling it to perform functions such as reading, storing, emulating, and writing to LF RFID cards.

Flipper Zero has a built-in RFID support with a low-frequency antenna located at the back of Flipper Zero. The STM32WB55 microcontroller unit is used for the 125 kHz RFID functionality.




125 kHz RFID hardware

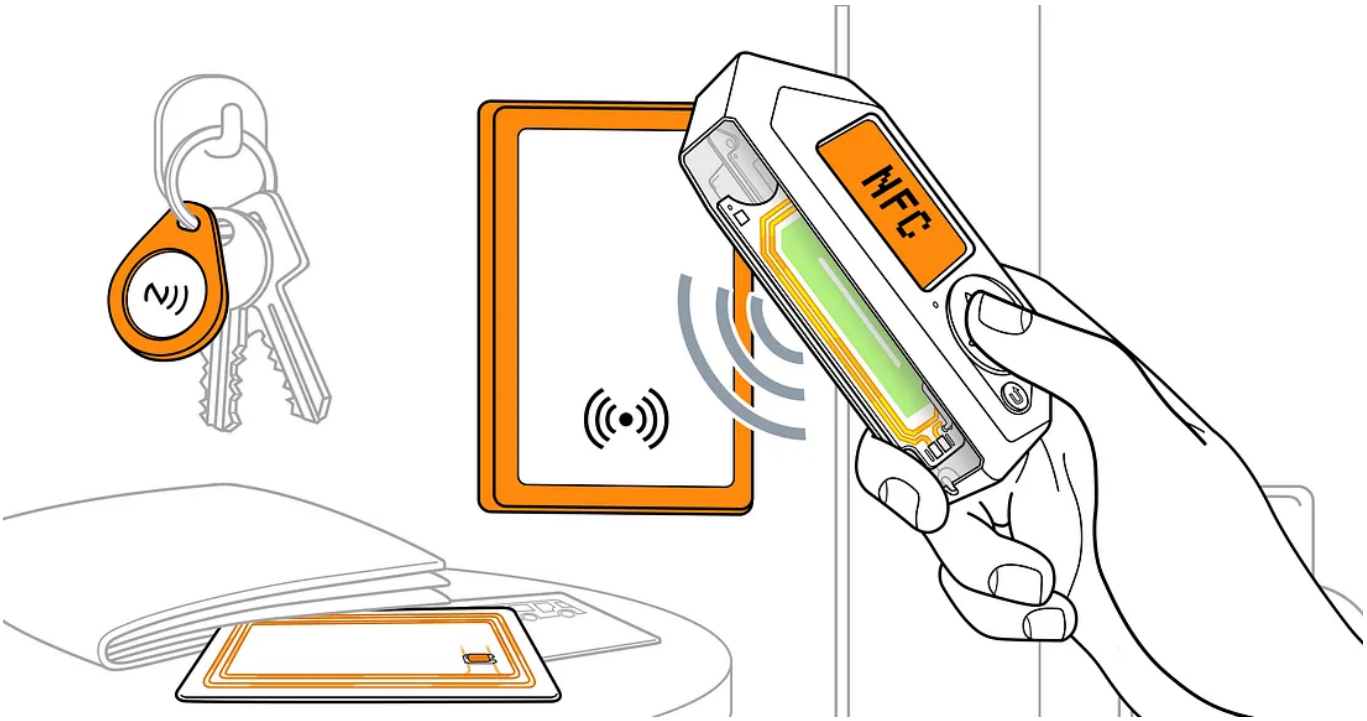
The low-frequency 125 kHz antenna is placed on the Dual Band RFID antenna next to the high-frequency 13.56 MHz antenna.




Dual Band RFID antenna

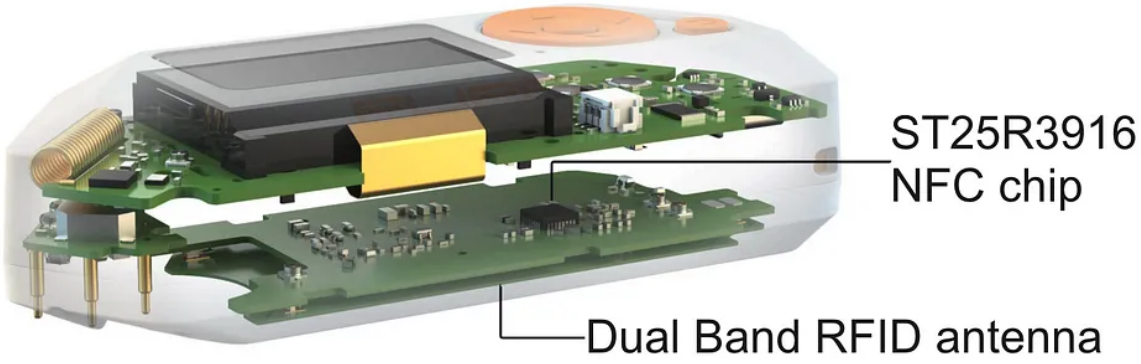
## NFC

https://docs.flipper.net/nfc



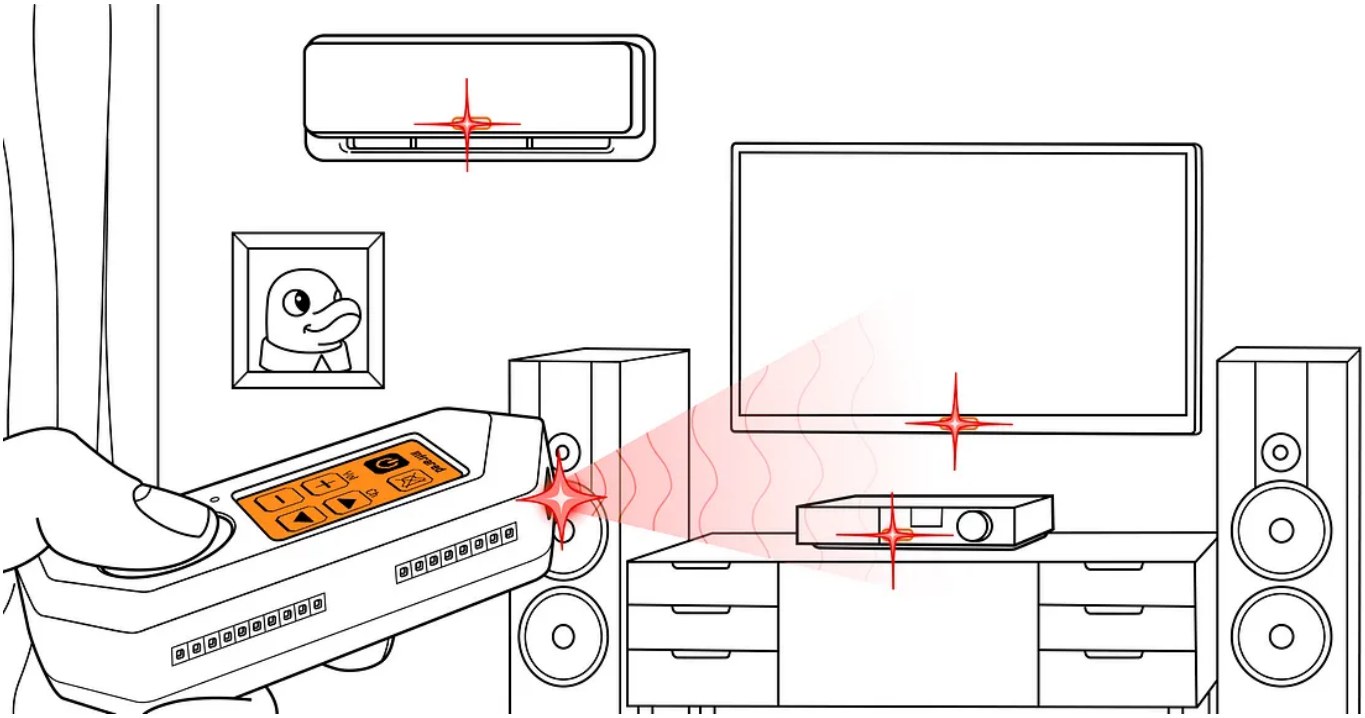
Flipper Zero is equipped with Near Field Communication (NFC) technology, widely used in various applications such as **smart cards for public transportation, access control cards or tags, and digital business cards.** These cards often involve intricate protocols and provide features like encryption, authentication, and **comprehensive two-way data exchange.** The device incorporates a built-in NFC module operating at 13.56 MHz, which allows it to read, store, and replicate NFC cards.

Flipper Zero has a built-in NFC module based on a ST25R3916 NFC chip and a 13.56 MHz high-frequency antenna. The chip is used for high-frequency protocols and is responsible for reading and emulation of cards.



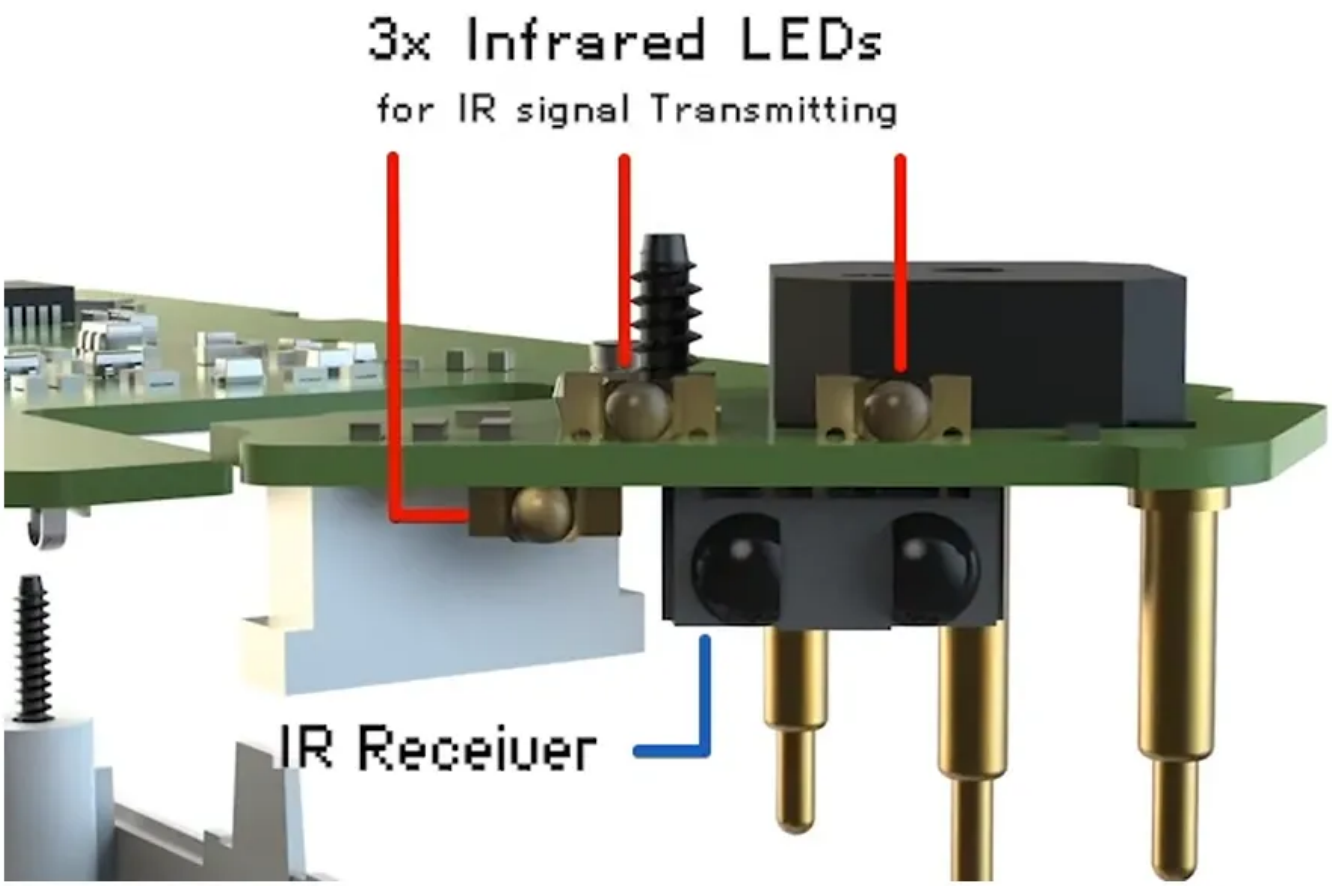

## Infrared

https://docs.flipper.net/infrared



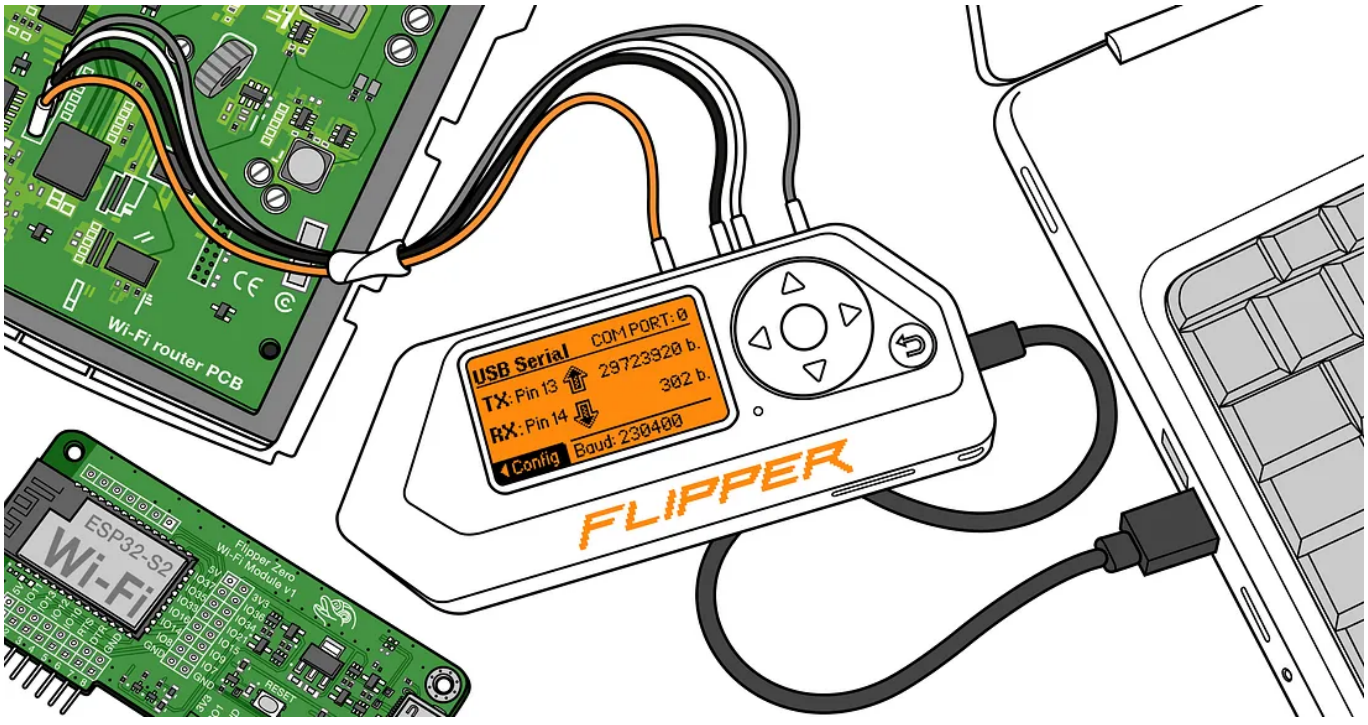
Flipper Zero is capable of interfacing with devices that communicate via infrared (IR) light, such as televisions, air conditioners, and multimedia systems. Thanks to its integrated infrared module, **the device can capture and store signals from infrared remotes, enabling it to function as a universal remote to control various devices.**

Flipper Zero has a built-in Infrared module consisting of an IR light transparent plastic window, three transmitting infrared LEDs, and a TSOP-75338TR infrared receiver.




## GPIO & modules

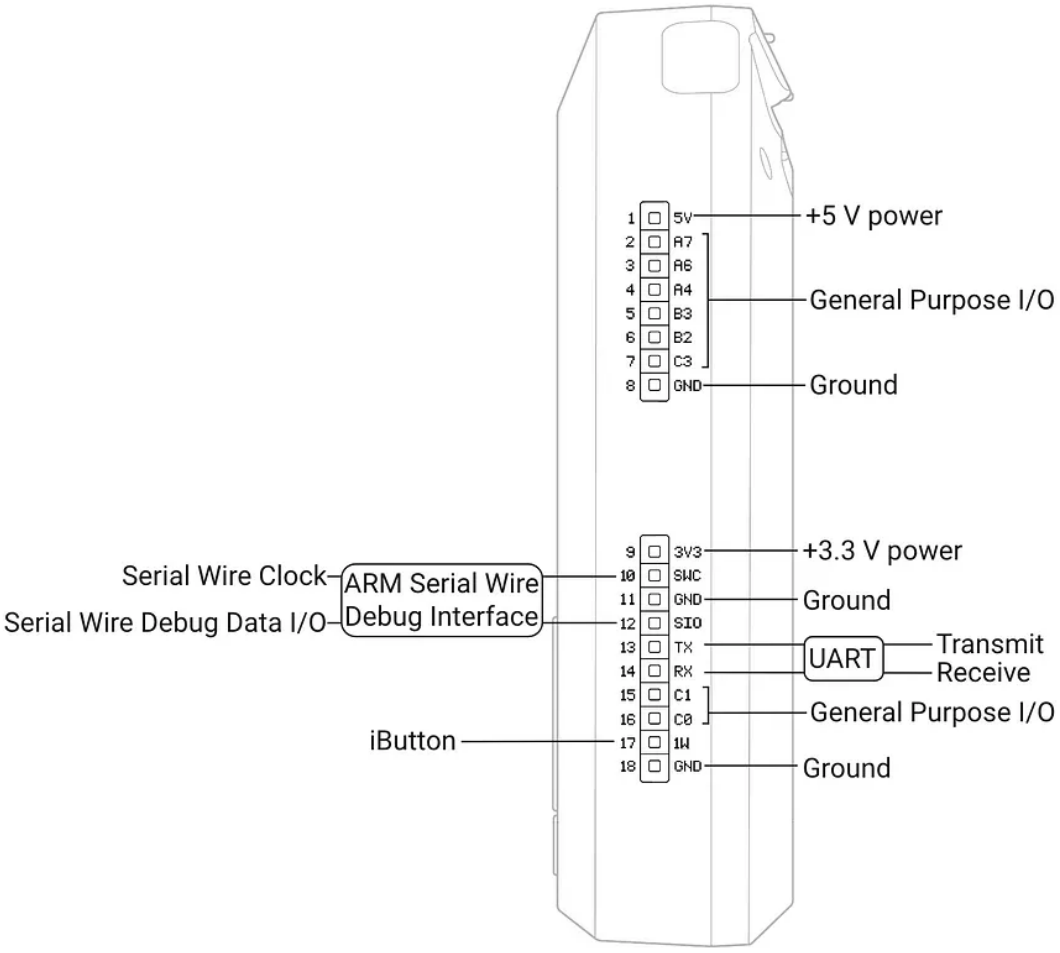
https://docs.flipper.net/gpio-and-modules



Flipper Zero serves as a versatile tool for **hardware exploration, firmware flashing, debugging, and fuzzing.** It can be linked to other hardware through its integrated GPIO pins, allowing you to manage hardware using its buttons, execute your custom code, and display debug messages on its screen. Additionally, Flipper Zero can function **as a converter for USB to UART/SPI/I2C interfaces.**

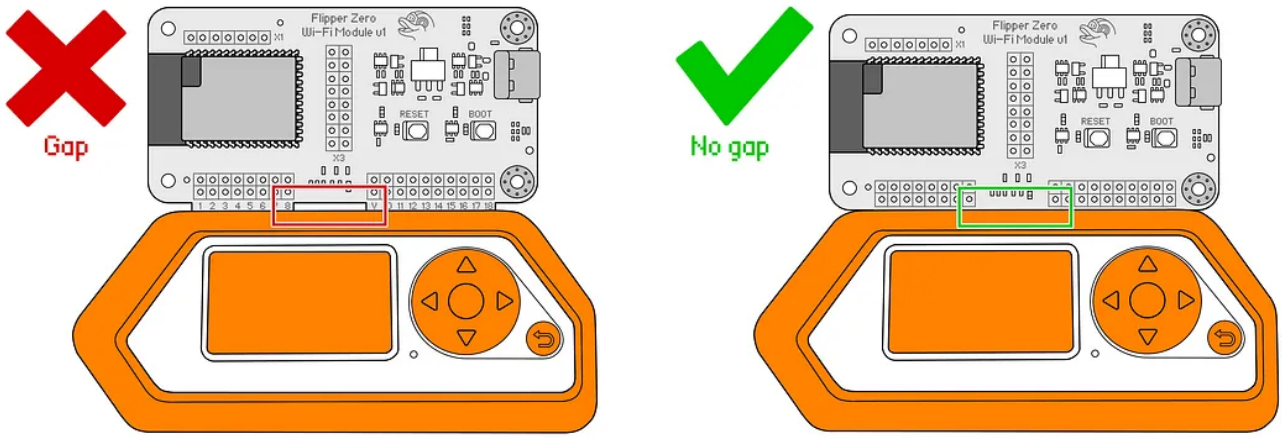
Flipper Zero has 18 pins on the top side, consisting of power supply pins and I/O pins. **Power supply pins** can be used to power your external modules. **Input/output (I/O) pins** are +3.3 V tolerant for input and output. For more information, see 3.3 V and 5 V tolerance.

I/O pins connect external modules to the I/O pins of the STM32WB55 microcontroller through 51 Ohm resistors. All pins are electrostatic discharge (ESD) protected. For information on the basic functionality of Flipper Zero pins, see the picture below.




Flipper Zero's pins

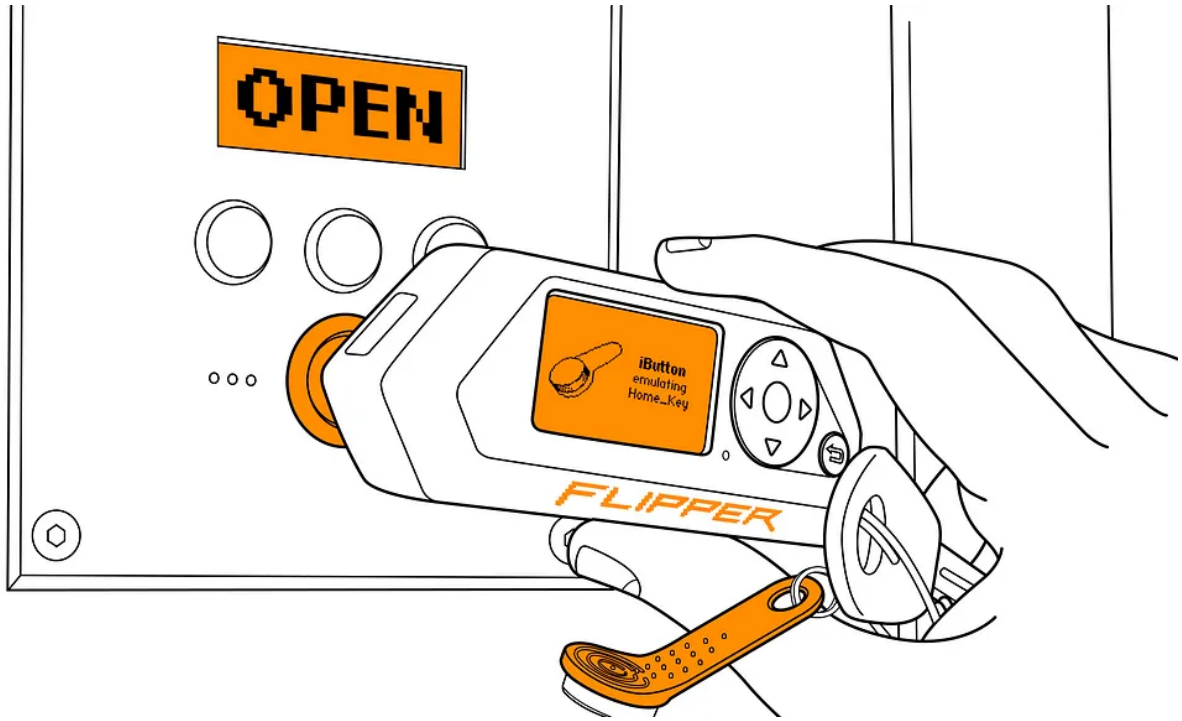
> *Note: If your **Flipper Zero is in a silicone case**, insert the module all the way in, so there is no gap in the middle between the silicone case and the module.*




Make sure there is no gap in the middle

## iButton

https://docs.flipper.net/ibutton

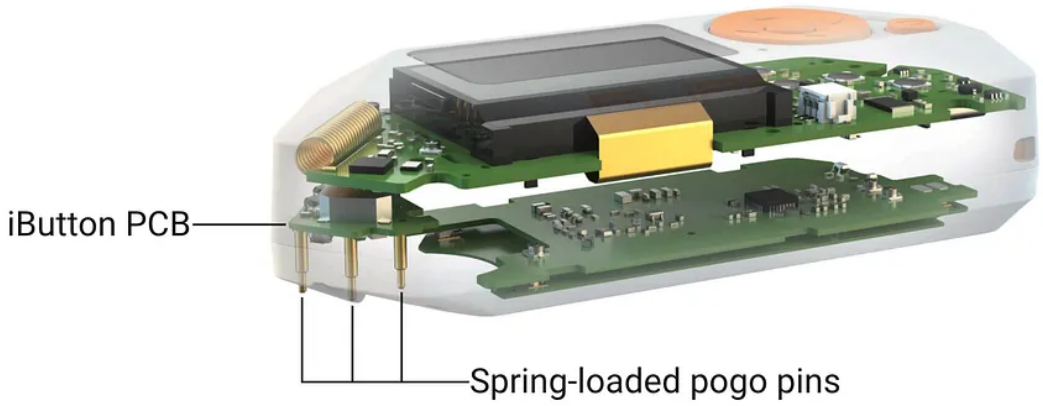



Flipper Zero is compatible with the 1-Wire communication protocol, often used in compact electronic keys, commonly referred to as iButton keys. These keys have **a range of applications, including access control, temperature and humidity measurements, and storage of cryptographic keys.**

Equipped with an integrated iButton module, Flipper Zero is adept at **reading, writing, and emulating iButton access control keys.** This module is versatile, supporting key protocols such as Dallas, Cyfral, and Metakom.

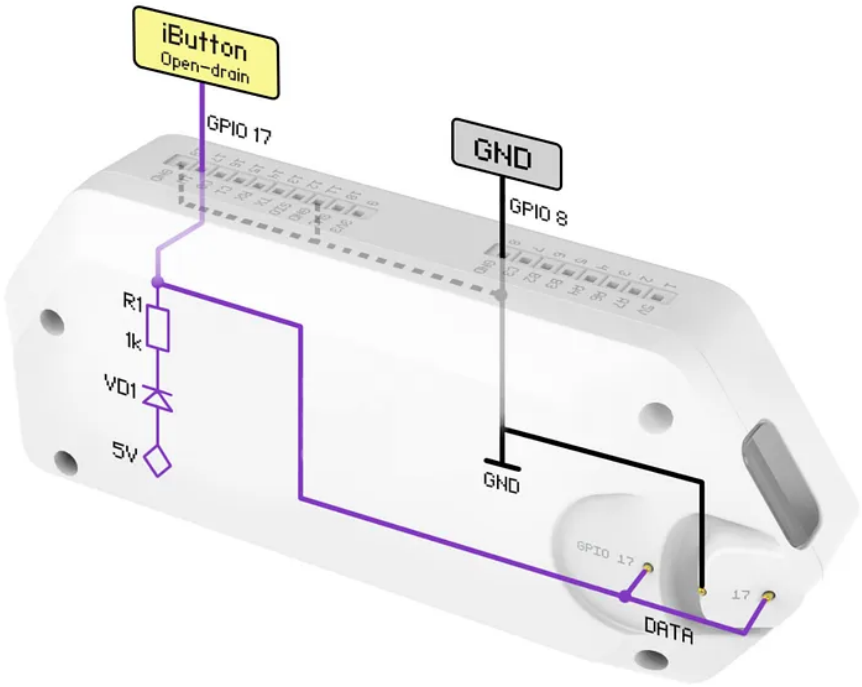
> *Note: Not all iButton devices can be detected by Flipper Zero*
> *Various iButton devices may have the same form factor, however, only access control keys can be detected by Flipper Zero.*

Flipper Zero has a built-in iButton module consisting of an iButton pad and three spring-loaded pogo pins that are located on the iButton PCB.



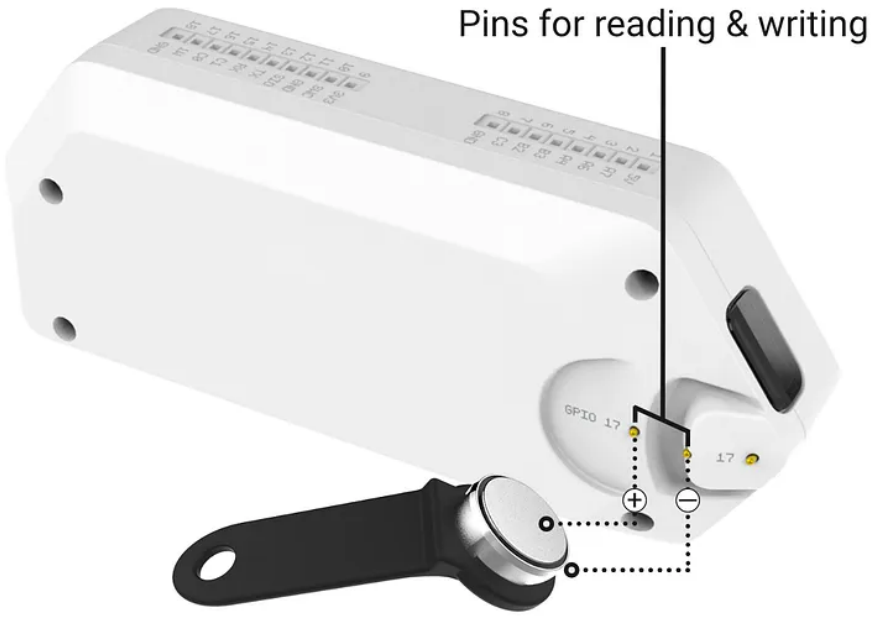

iButton module's pins

Two pins are assigned to data transfer and have output to the GPIO pin 17. The remaining middle pin is ground.



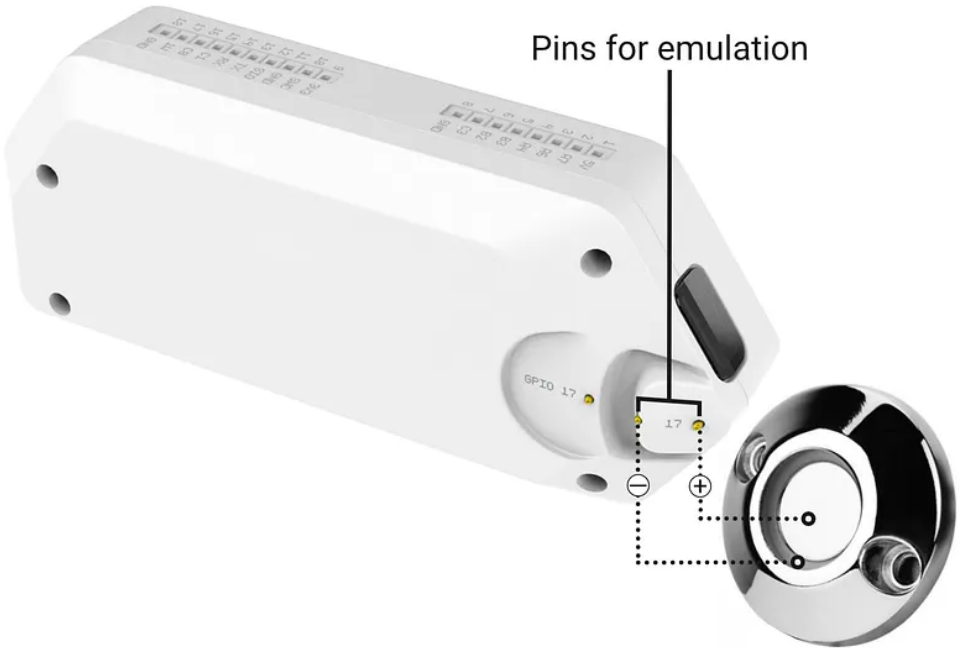

iButton data pins have output to the GPIO pin 17

The flat part of the pad allows connecting an iButton key (Slave) with Flipper Zero (Master). The left data pin and the middle ground pin are used for reading and writing iButton keys.




Pins used for reading and writing

The protruding part of the pad allows connecting Flipper Zero (Slave) with an iButton reader (Master). The right data pin and the middle ground pin are used for emulation of iButton keys.




Pins used for emulation

## Bad USB

https://docs.flipper.net/bad-usb

Flipper Zero has the capability to function as a BadUSB device, which computers identify as a Human Interface Device (HID), similar to a keyboard. As a BadUSB, **it can modify system settings, open backdoors, extract data, initiate reverse shells, or perform any task achievable through physical access.** This is executed through a series of commands written in Rubber Ducky Scripting Language, commonly known as DuckyScript. These specific commands are referred to as a payload.

- **Flipper Zero scripting language**

Before using your Flipper Zero as a BadUSB device, you need to write a payload in the .txt format in any common ASCII text editor using the scripting language. Flipper Zero can execute extended Rubber Ducky script syntax. The syntax is compatible with the classic Rubber Ducky Scripting Language 1.0 but provides additional commands and features, such as the ALT+Numpad input method, SysRq command, and more.

Both \n and \r\n line endings are supported. Empty lines are allowed, as well as spaces or tabs for line indentation. The Bad USB application can execute only scripts in the .txt format. No compilation is required.

- **Uploading new payloads to your Flipper Zero**

Once the payload is created, you can upload it to your Flipper Zero via qFlipper or Flipper Mobile App to the SD Card/badusb/ folder. The new payloads will be available in the Bad USB application.

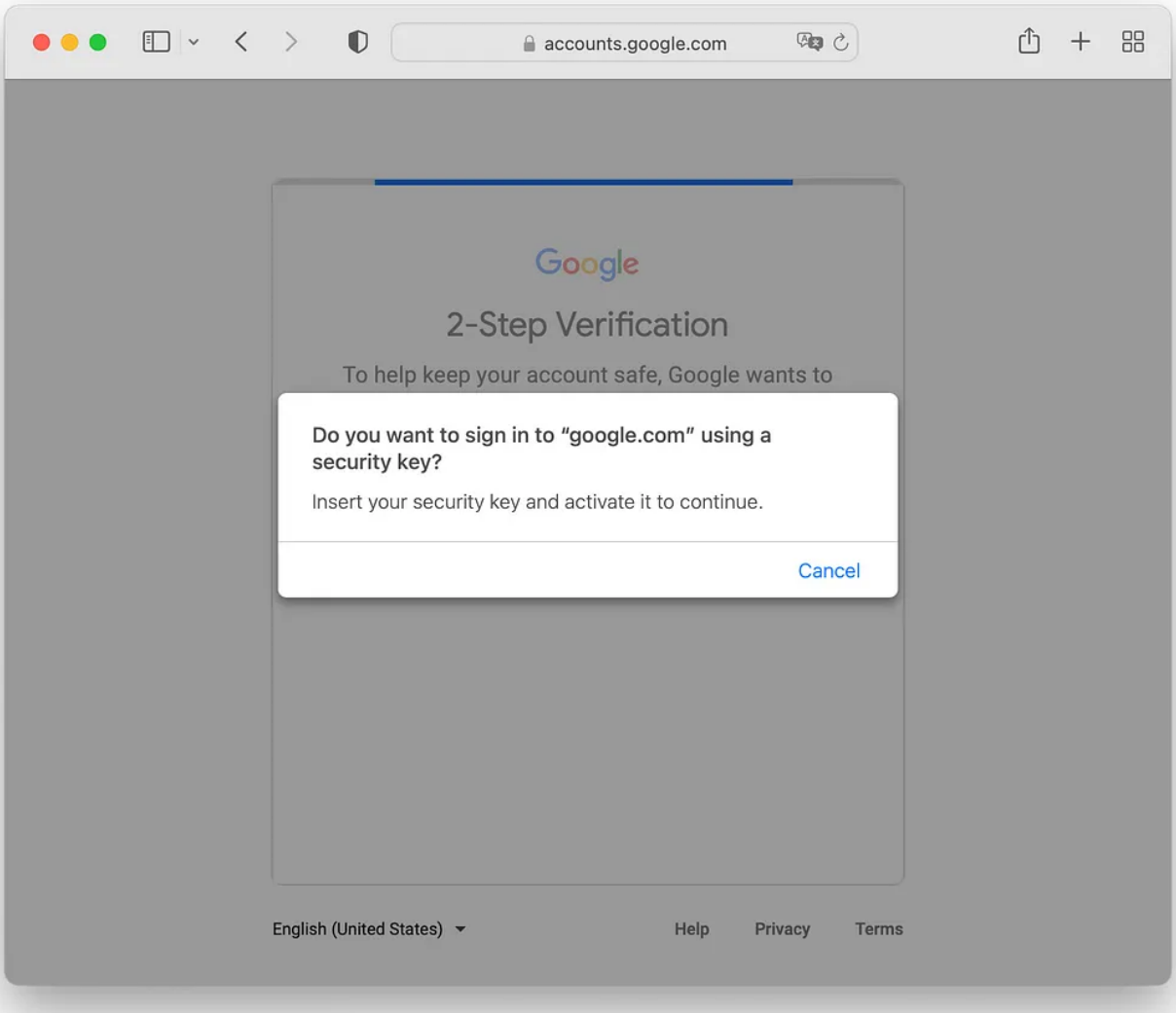

> *Note: When uploading, files with the same names will be overwritten without warning.*

### U2F (Universal 2nd Factor)

https://docs.flipper.net/u2f

**Flipper Zero can act as a USB universal 2nd-factor (U2F) authentication token or security key that can be used as the second authentication factor when signing in to web accounts.** A security key is a small device that helps computers verify that it is you when signing in to an account. The use of this feature increases the security of your accounts.

- **Signing in with your Flipper Zero**




> *Note:* ***Do not delete, edit, or move U2F files to another Flipper Zero***

> *Each Flipper Zero has a unique cryptographic key that generates unique encrypted U2F files. If you reinsert your microSD card with U2F files into another Flipper Zero, you'll not be able to sign in to your web accounts with the new device.*
>
> *If you delete U2F files, edit U2F files, or insert a new microSD card into your Flipper Zero, the device will generate a new set of U2F files. In this case, you'll be required to re-register Flipper Zero as a security key in all of your web accounts.*
>
> *If you delete the `u2f/assets` folder or the `u2f` folder entirely, your Flipper Zero will not be able to use the U2F application, as the assets folder contains the cryptographic certificate that is used for registration and authentication. You can restore this folder by updating your Flipper Zero's firmware.*

## Apps

https://docs.flipper.net/apps

The Apps catalog is a collection of tools and games created by the Flipper Zero community. This diverse range of apps enhances the functionality of Flipper Zero, **making the user experience with the device even more gamified and enjoyable.**

Access to the Apps catalog is available through the Flipper Mobile App and Flipper Lab, which are compatible with Google Chrome, Microsoft Edge, and other Chromium-based browsers that support the Web Serial API.

## Section 3: Hands-on with Flipper Zero

### 3.1 Step-by-step guides for Common Use Cases seen in the wild.

#### 3.1.1 Capturing and replaying Sub-GHz signals such as signals from Garage Door Remotes

Reference: Derek Jamison's YouTube Channel — https://www.youtube.com/@MrDerekJamison

> *IMPORTANT DISCLAIMER:*
>
> *- These guides are for EDUCATIONAL PURPOSES ONLY.*
>
> *- Never bypass an access control or unlock anything you do not own or have not given permission from the owner to access or unlock.*
>
> *- Never try to fuzz or replay signals to devices that are in use or that you rely on.*
>
> *- Please don't try this guide on car keyfobs that you rely on because you risk desynchronizing your key, or damaging the receiver and ending up paying a lot of money to restore it.*

### Simple Remotes (No Rolling Codes)

1. Use the Sub-Ghz module.
2. Go to “Frequency Analyzer” option to determine the exact frequency the remote is working (example: 433.88 MHz). Push the button of the remote and the frequency will be displayed in the Flipper Zero screen.
3. Go to “Read Raw” option and push the LEFT button to edit the configuration.
4. Set the frequency to 433.92 Mhz. Note: this is the closest option to the “433.88MHz” result we got from the “Frequency Analyzer”, don’t expect to find an exact match from the frequency analyzer.
5. Set the “RSSI Threshold” to -75.0
6. Press BACK go to the Read Raw screen
7. Press REC and then press the button from your remote.
8. Press Stop.
9. Press RIGHT button to Save the recording and give it a name.
10. Navigate to “Saved” Signals. Choose the one you named in the previous step.
11. Go near to the your Garage Door and press SEND button.
12. Enjoy!

### More complex Remotes (Use of Rolling Codes)

1. Take the remote somewhere out of range so it can’t communicate with the receiver (garage door). Our goal is to press the button on the remote and capture the signals without the signals actually making their way to the receiver.

2. Repeat steps 1–11 from above.
3. Remember that each captured signal will only work once with the receiver on your Garage Door.

**Why should you care about this type of attack?**

There are many products selling online currently that are susceptible to replay attacks and don't even offer basic protection mechanisms such as rolling codes. Being able to assess your own hardware before actually using it as a home appliance can dramatically improve you home security posture.

### 3.1.2 Use the Flipper Zero as a BadUSB — Emulate a keyboard

Recommended resources for this type of attack:

- Flipper Zero Xtreme Firmware — https://github.com/Flipper-XFW/Xtreme-Firmware
- https://github.com/Zarcolio/flipperzero
- https://www.youtube.com/watch?v=G9wTr5EOxpU
- https://github.com/FalsePhilosopher/badusb
- https://www.reddit.com/r/FlipperZeroDev/comments/zxcy84/badusb_payloads/
- https://github.com/aleff-github/my-flipper-shits/

### 3.1.3 RFID Fuzzing with Flipper Zero

Reference: https://www.youtube.com/watch?v=EcWTFZovNTE

1. Install the RFID phaser app from the app store onto your Flipper Zero device.

2. Familiarize yourself with the Flipper Zero's functionality and interface.
3. Choose from four popular low-frequency protocols available in the app. These should match or be relevant to the system you are testing.
4. Understand the protocols: EM4100, HID, Indala, and T55xx.
5. Configure two critical values in the app. Time Delay (TD): The idle time between UID submissions. Emulation Time (EMT): The transmission time of one UID. For the example in the video, set TD to 0.4 and EMT to 0.5.
6. Select the mode of operation within the app. Options include: Default values (using the app's dictionary), BF Customer ID (iterates over selected byte), Load file (from Flipper format key file), Load custom IDs (from SD card).
7. Use Default Values and fuzzing list.
8. Observe the system's response to the fuzzing. Look for any irregularities or unexpected behaviors.
9. Identify if the system enters a 'weird state' allowing unauthorized access.
10. Experiment with different cards (right and wrong) to test the system's reaction.
11. Finish the batch of tests and check if the system's state has changed.
12. Confirm if a wrong card is now accepted as a right card, indicating a successful fuzz.

### Understanding Limitations and Ethical Use

Recognize the limitations of RFID fuzzing, including time consumption, potential for not finding all vulnerabilities, expertise needed, false positives, hardware/software limitations, and the necessity of physical proximity.

### 3.1.4 Exploiting Insecure NFC Cards used with Access Controls with Flipper Zero

Reference: https://www.youtube.com/watch?v=hZMU4kPJ_zQ

**Gear:**

Gather different types of NFC cards/tags: an official UniFi Access NFC card, a UV key, and a cheap NTAG 215 tag.

**Process:**

1. On your Flipper Zero, navigate to the NFC function and select 'Read'.
2. Test reading the official UniFi Access card. Note that it reads as an unknown ISO tag, displaying the UID.
3. Try to emulate the UID of the official UniFi card and the UV key using Flipper Zero.
4. Observe that the system does not respond to these emulations, indicating a level of security.
5. Read the NTAG 215 tag using Flipper Zero, which identifies it correctly.
6. Use Flipper Zero to emulate the NTAG 215 tag.
7. Test this emulation with the UniFi Access system and observe that it grants access.

### 3.1.5 Turn on/off or interact with Screens or HVAC Systems to Create distractions or meet you objectives during a Red Team Engagement

**Objective:**

The primary goal in a red team exercise might be to test the physical security measures, response protocols, and the overall resilience of an organization against intrusion or security breaches. By interacting with screens or HVAC systems, a red team can assess how staff respond to unexpected changes or distractions, and how quickly they can identify and rectify such situations.

How Flipper Zero Comes into Play:

1. **Interacting with Screens:**

- Digital Signage and Monitors: Many modern offices and facilities use digital signage or monitors for information display, alerts, or advertisements. Flipper Zero, with its ability to transmit various signals (like infrared), can be used to change the content being displayed, switch screens on or off, or otherwise manipulate these devices.
- Creating Distractions: By changing what's displayed on screens or turning them off, the red team can create distractions. This can help in assessing how staff members react to unexpected technical issues or how they follow protocols in such situations.

**2. Manipulating HVAC Systems:**

- Temperature and Airflow Changes: HVAC systems in a building can often be controlled remotely. With Flipper Zero, you might be able to interact with these systems to change temperature settings or airflow, creating a noticeable environmental change.
- Testing Responses to Environmental Changes: By altering the HVAC settings, the red team can evaluate how staff respond to discomfort or unexpected changes in the environment. This could be crucial in

understanding the preparedness of the facility management team and the effectiveness of their response strategies.

**Scenario Execution:**

- The red team would use Flipper Zero to identify and interact with the signal systems of screens and HVAC controls.
- Once access is gained, they would execute predefined actions like turning off screens, displaying alternative content, or adjusting HVAC settings.
- The team would then observe and record how the staff and security personnel react to these changes. Do they investigate the issue? How long does it take them to respond? Do they follow established protocols?

### 3.1.6 Read, Write and Emulate DS199A, Cyfral, and Metakom protocols for iButtons. These keys are used for access control, temperature measurements, humidity measurements, storing cryptographic keys, etc.

Reference: https://www.youtube.com/watch?v=q8CFM4_mgS0

**Step 1: Reading an iButton**

- Select 'Read' and bring the iButton into contact with the two captors on the back of the Flipper Zero.
- Ensure one captor touches the side and the other the middle part of the iButton.

**Step 2: Saving iButton Data**

- After reading, press ‘More’ for additional options and select ‘Save’ to store the iButton data.
- Name the dump for future reference, emulation, or writing.

**Step 3: Emulating an iButton**

- Choose the ‘Emulate’ function to make Flipper Zero act as the iButton.
- Keep the captors in direct contact with the iButton reader during emulation.
- Verify the emulation accuracy by comparing with the original iButton.

**Step 4: Writing to an iButton**

- Select ‘Write’ to copy the data onto a writable iButton.
- The Flipper Zero will vibrate to indicate successful copying.
- Verify the copied iButton to ensure accuracy.

**Step 5: Adding iButton Data Manually**

- Choose ‘Add Manually’ to input an iButton key directly.
- Select the appropriate protocol and manually enter the key.

**Step 6: Managing Saved iButton Data**

- Go to ‘Saved’ to access previously stored iButton dumps.
- For each dump, you have options to emulate, write, edit, delete, or get more information.

- Editing allows modification of the keys, while information provides details like the protocol used.

**Basic Flipper Zero iButton Workflow Examples**

- Example 1 (Read and Save): Read an iButton, save the dump, name it for later emulation or copying.
- Example 2 (Emulate iButton): Either read an iButton and emulate it or use a saved dump for emulation.
- Example 3 (Copy iButton): Open a saved dump, select 'Write,' and copy the data onto a writable iButton.

Advanced iButton Use Case Scenario — Emulate and Bruteforce Dallas iButton DS1990A

- YT Video link: https://www.youtube.com/watch?v=tt1bnbN87Nw

### 3.2 Video Links with Common Flipper Zero Attacks

- **Apple BLE Spam** — https://www.youtube.com/watch?v=pD8jze5fCHA
- **iOS 17 Lockup Crash** — https://www.youtube.com/watch?v=7FPx5L3xsdU
- **Open Garage Doors** — https://www.linkedin.com/posts/rapper_this-is-how-a-hacker-can-access-your-house-activity-7149523721018376193-6KnJ?utm_source=share&utm_medium=member_desktop
- **Hacking Gas Prices** — https://www.youtube.com/watch?v=wtHr7x_wT40
- **Controlling Traffic Lights** — https://www.youtube.com/watch?v=wtHr7x_wT40

- **Replaying Car Key Fobs Rolling Codes —** https://www.youtube.com/watch?v=SVmxhTl49SY
- **Flipper Zero Jamming Signals —** https://www.youtube.com/watch?v=aHXx3niWDnY
- **Wireless Mouse and keyboard Hijacking Flipper Zero —** https://www.youtube.com/watch?v=actbJx7oEZU
- **Flipper Zero Hacking in Public Compilation —** https://www.youtube.com/watch?v=u1GDUapHdUw

## Section 4: Extending Functionality

### 4.1 Customizing the Firmware of Flipper Zero

Two of the most popular and feature-rich firmware are the following:

1. **Xtreme Firmware:** This firmware is known for being feature-rich, stable, and customizable. It includes a wide array of apps, an extensive reservoir of features, and offers high stability due to the rewriting of most core parts of the firmware. Additionally, it provides significant customization options, allowing users to change animations, icons, the Flipper's name, level, or mood directly on the device. Key features include asset packs for easy installation and switching between animation and icon sets, expanded Bluetooth functionality, support for many protocols including rolling code devices, a completely redesigned interface, and an advanced level system. Link: https://github.com/Flipper-XFW/Xtreme-Firmware , Installation: https://www.youtube.com/watch?v=Zj_PWkWxUEw
2. **Unleashed Firmware:** The Flipper Zero Unleashed Firmware is another popular choice, characterized by its extensive list of features and strong community support. Link: https://github.com/DarkFlippers/unleashed-

firmware , Installation: https://www.youtube.com/watch?v=THnMSSXC3mo

### 4.2 External Plugins and Resources

1. **Awesome FlipperZero Collection:** A comprehensive collection of resources for the Flipper Zero device, including various scripts, tools, and applications. Link: https://github.com/djsime1/awesome-flipperzero
2. **Flipper Zero WiFi Scanner Module:** A module for FlipperZero based on ESP8266/ESP32, designed for scanning WiFi networks. Link: https://github.com/SequoiaSan/FlipperZero-WiFi-Scanner_Module
3. **FlipperZero-Wifi-ESP8266-Deauther-Module:** A module that performs WiFi deauth attacks using ESP8266. Link: https://github.com/SequoiaSan/FlipperZero-Wifi-ESP8266-Deauther-Module
4. **FlipperZero IR Xbox Controller:** This plugin enables Flipper Zero to function as an IR controller for Xbox. Link: https://github.com/gebeto/flipper-xbox-controller
5. **Flipper Zero Barcode Scanner Emulator**: Emulates a barcode scanner for testing cash registers, demonstrating the versatility of Flipper Zero in various practical applications. Link: https://github.com/polarikus/flipper-zero_bc_scanner_emulator
6. **Custom Animations and Graphics:** There are various plugins and resources available for customizing Flipper Zero with unique animations and graphics. These include Lab401 Animation Video, Kuronons Graphics, Flipper Animation Manager, zip2Animation utility, H4XV's Gif2Anim Converter, and more. Link: https://github.com/Kuronons/FZ_graphics

7. **Modules and Cases:** There are several 3D printable cases and modules available for Flipper Zero, enhancing its functionality and customization. Examples include the Ultimate Flipper Zero Case, FlipperZero-Hardware 3D-Printable cases, WiFi Scanner Module, and WiFi Deauther Module Flasher.
8. **Off-device & Debugging Tools:** Various tools and scripts are available for managing Flipper Zero animations, converting file formats, and debugging applications. These include the Official Web Interface, csv2ir script, Marauder for Wifi Dev Board, and Flipper File Toolbox.

## Section 5: Resources

### 5.1 References and Additional Resources

- **Flipper Zero Documentation**

Official Documentation, https://docs.flipper.net/

HackTricks, https://book.hacktricks.xyz/todo/radio-hacking/flipper-zero

- **Flipper Zero Popular Communities**

Reddit, https://www.reddit.com/r/flipperzero/

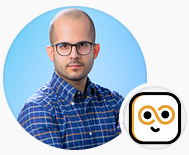
Discord, https://discord.com/invite/y5E5m8jbgb

Official Flipper Forum, https://forum.flipper.net/

### 5.2 Additional Hardware for Flipper Zero

- **External CC1101 Antenna for Flipper Zero — Sub-Ghz GPIO Board Attachment —** https://www.reddit.com/r/flipperzero/comments/13a31wz/external_cc1101_antenna_for_flipper_zero_subghz/

Hacking Tools | Flipper Zero | Cybersecurity | Penetration Testing | Technology



## Written by Ilias Mavropoulos

Follow

131 Followers · Writer for InfoSec Write-ups

Global SOC Red Team Operator, Penetration Tester | Accredited eJPT, Gold Coin BTL1, ISC2 Certified in Cybersecurity (CC) and 7 more | MS Cybersecurity

### More from Ilias Mavropoulos and InfoSec Write-ups


Ilias Mavropoulos in InfoSec Write-ups

## Mastering BTL1: Journey, Tips, and Insights for Cyber Defenders

Discover the BTL1 certification journey, learn valuable tips, and gain insights into the...

9 min read · Apr 4, 2023

93 2

SynapticSpace in InfoSec Write-ups

## How I made 7K on Epic Games Bug Bounty

I escalated a low impact vulnerability to a critical one and received 7K! Let me show yo...

8 min read · Dec 28, 2023

537 6

YASHH in InfoSec Write-ups

## Master Subdomain HUNTING | Art of finding Hidden Assets

Hey guys it's Yash Again, Today we are going to learn about Importance of Subdomain...

3 min read · Dec 29, 2023

310 3


Ilias Mavropoulos in InfoSec Write-ups

## eJPT v2 Review: Decoding the eLearn Security's Junior...

Your Gateway to Ethical Hacking: A Comprehensive Look at eJPT v2.

8 min read · Sep 5, 2023

36 1

See all from Ilias Mavropoulos | See all from InfoSec Write-ups

## Recommended from Medium

James Presbitero Jr. in Practice in Public

### These Words Make it Obvious That Your Text is Written By AI

These 7 words are painfully obvious. They make me cringe. They will make your reader...

4 min read · Dec 31, 2023

20K 583


Manish Singh

### How I Passed OSCP 2023 in Just 8 Hours with 110 Points Without...

Hey everyone, If you've ever been curious about how to pass OffSec Certified...

10 min read · Aug 17, 2023

692 8

## Lists

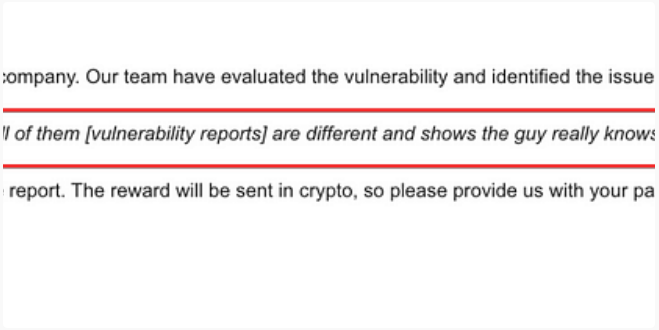
**AI Regulation**
6 stories · 281 saves

**ChatGPT prompts**
34 stories · 994 saves

**Generative AI Recommended Reading**

**ChatGPT**
23 stories · 404 saves

52 stories · 638 saves



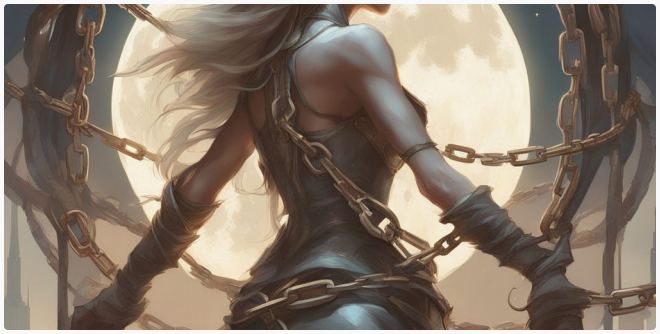

Manav Bankatwala in InfoSec Write-ups

## 1 Program, 4 Business Logic Bugs and Cashing in 2300$.

Not every time coding is necessary in cybersecurity.

6 min read · 4 days ago

337 6



Batuhan Aydın

## Hacking Mindset— You Need to Learn These

Hello folks, I am with you again in an article. The topic of today's article is a topic that is...

9 min read · Jan 9

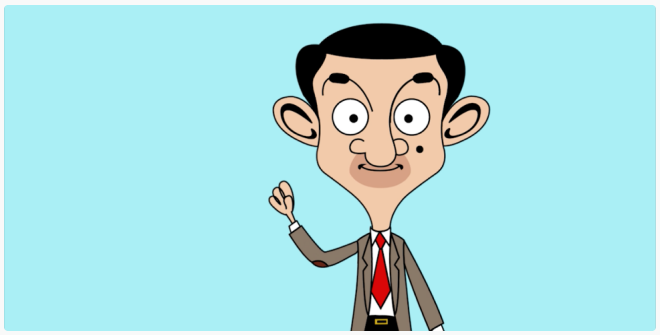
321 11

Financeable

## 12 Side Hustles You Can Do From Your Phone ($600+ Per Day)

Let's be honest, if you're reading this article, you probably have a phone or a laptop. And...

13 min read · Dec 25, 2023



Samet Yiğit

## My first bugs in 2024

Hello everyone, In this article, I will explain how I found 4 bugs from a program in...

3 min read · Jan 5