

# Flipper Zero

Ricardo L0gan

## ❖ Agenda



- 0x00 - **Motivation** of Research
- 0x01 - Disassemble Flipper
- 0x02 - News About Flipper
- 0x03 - Demos
- 0x04 - Conclusion
- 0x05 - Reference



# 0x00 - Motivation of Research



Hak5 rubber ducky



HackRF One



Hak5 wifi pineapple



Hardware Hacking

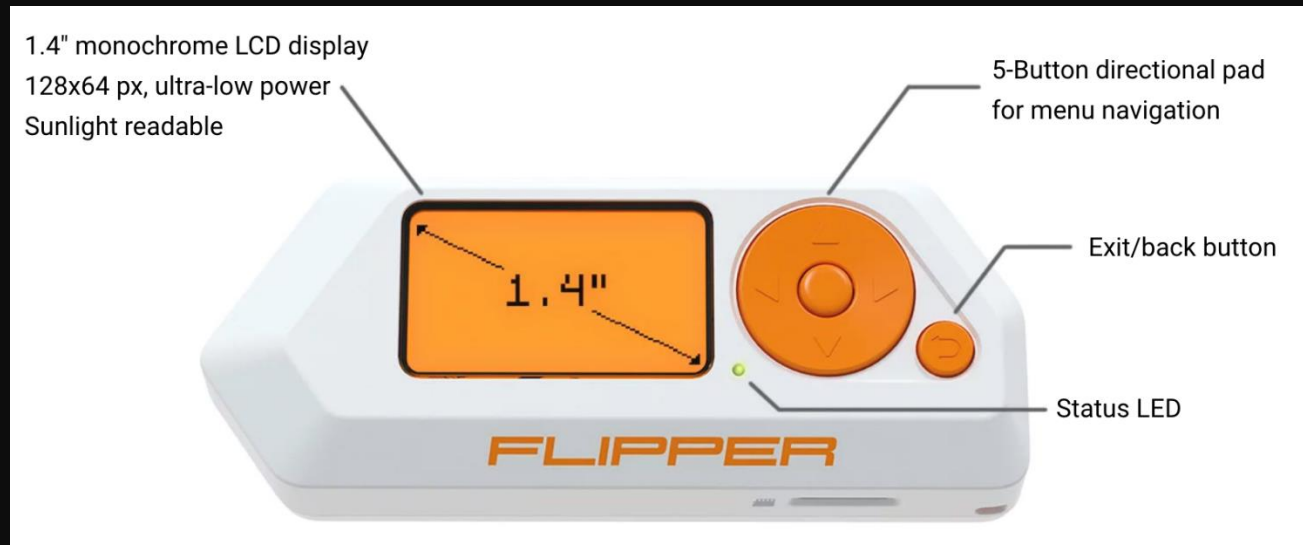
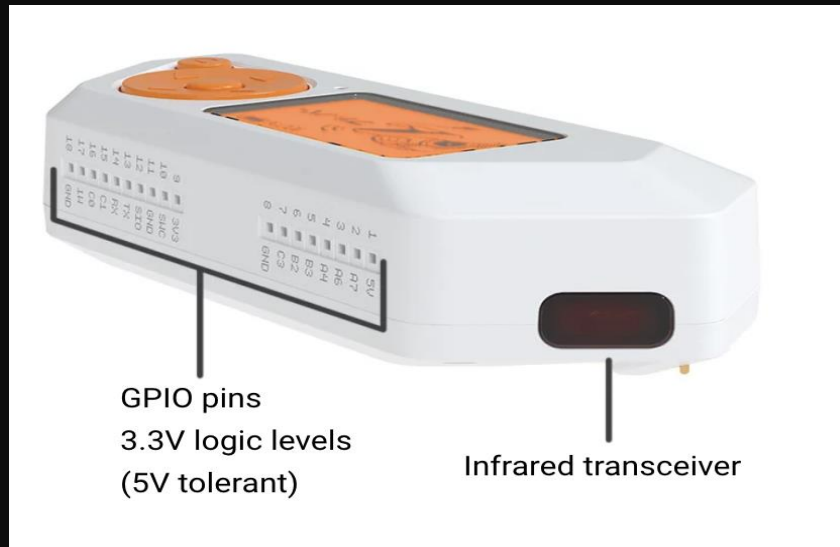
## 0x00 - Motivation of Research



Criado por Alex Kulagin e Pavel Zhovner  
KickStarter 2019

Flipper is Based on ultra low power STM32 ARM MCU for daily exploration of access control systems and radio protocols, Open source and customizable.

# 0x01 - Disassemble Flipper

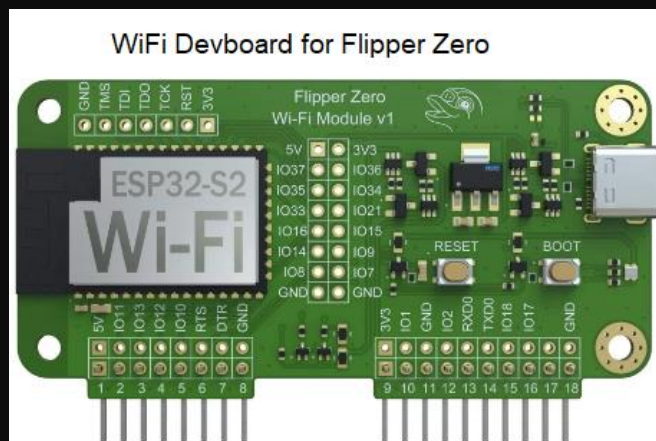




# 0x01 - Disassemble Flipper



		
FLIPPER DEVICES	FLIPPER DEVICES	FLIPPER DEVICES
R\$118.40	R\$70.30	R\$87.40
★★★★★	★★★★★	★★★★★
Flipper Zero silicone cover	Flipper Zero protective glass	Prototyping Boards for Flipper Zero



Fonte: <https://www.joom.com>

# 0x01 - Disassemble Flipper



## 125 kHz RFID

Low frequency proximity cards. Reading, writing and emulating 125 kHz RFID tags.



## NFC

High frequency 13,56 MHz smart cards. Reading, attacking, writing and emulating NFC cards.



## Sub-GHz

Radio systems under 1GHz frequency range. Manipulating digital wireless remotes and their radio protocols.



## Infrared

Infrared signals used in TVs, audio systems, air conditioners and more. Reading and emulating infrared remotes.



## Bad USB

Emulating PC keyboard to inject keystrokes via USB. Rubber Ducky's scriptable payloads language.



## U2F

USB universal 2nd-factor security key. Sign in to web accounts with Flipper Zero.



## GPIO & modules

General Purpose I/O pins for connecting hardware modules. Physical wired connection via UART, SPI, I2C.



## iButton

Dallas touch memory keys (1-Wire). Reading, writing and emulating iButton electronic keys requiring physical contact.



## Basics

How to Update Firmware, Control your device, Setup the SD card, edit Settings and recover in case of failures.



## qFlipper

Desktop application for the firmware update, file management, and firmware repair.



## Mobile apps

Flipper Android/iOS mobile apps provide extended control of the device: updating firmware, sharing keys and more.



## Development

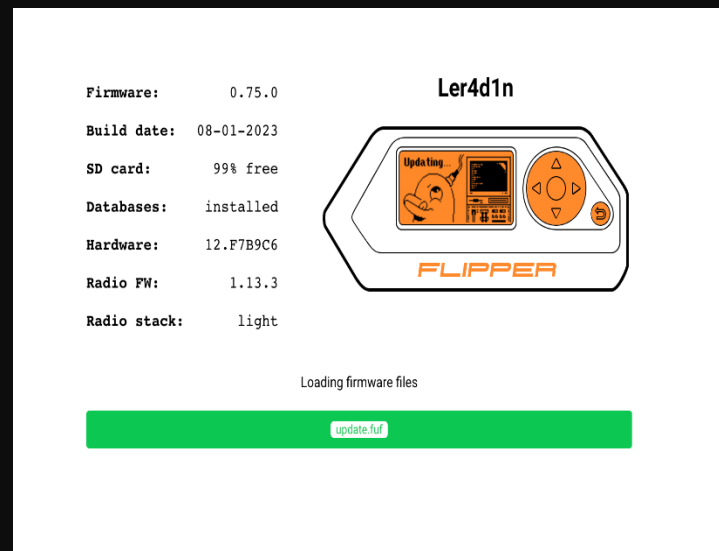
Software and Hardware development. System API's documentation, code examples, debugging, PCB schematics.



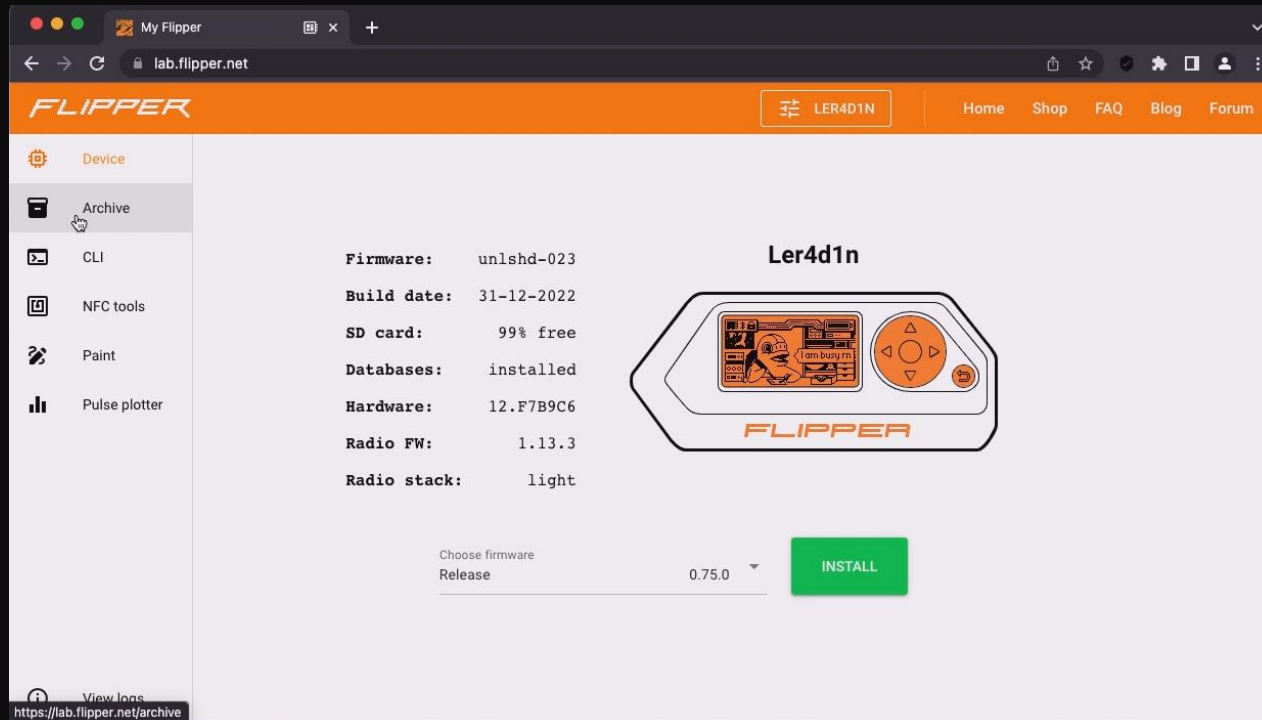
# 0x01 - Disassemble Flipper



# 0x01 - Disassemble Flipper



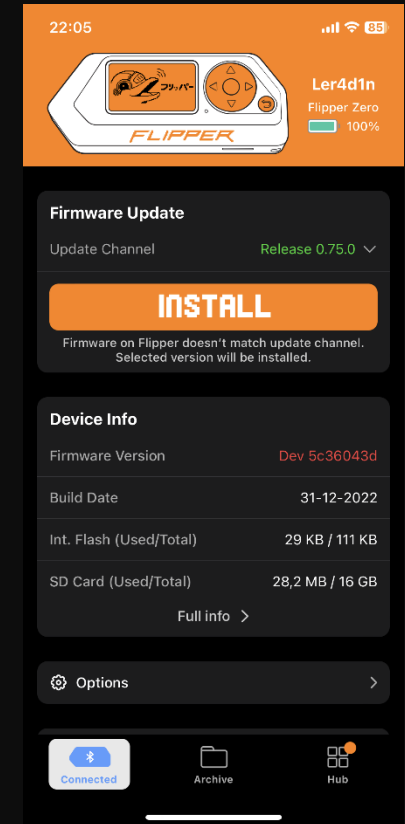
# 0x01 - Disassemble Flipper



Web Updater

<https://lab.flipper.net>

\*Melhor compatibilidade com Chrome



# 0x01 - Disassemble Flipper



## Levels:

- Level 1: 0 XP
- Level 2: 735 XP
- Level 3: 2940 XP

\* Maximum 15 xp points each categories and 105 xp per day with All Categories.

### •Sub-Ghz

- Enter Read Screen: 1 XP
- Save a Signal: 3 XP
- Record Raw: 1 xp
- Add signal manually: 2 XP
- Send Saved Signal: 2 XP
- Frequency Analyzer: 1 XP

### •125Khz

- Enter Read Screen: 1 XP
- Read Success: 3 XP
- Save a signal: 3 XP
- Emulate Signal: 2 XP
- Manual Add: 2 XP

### •NFC

- Enter Read Screen: 1 XP
- Read Success: 3 XP
- Save NFC: 3 XP
- Emulate NFC: 2 XP
- Manual Add NFC: 2 XP

### •Infrared

- Send IR Signal: 1 XP
- Learn Success: 3 XP
- Save IR: 3 XP
- Brute Force IR: 2 XP

### •iButton

- Enter Read Screen: 1 XP
- Read Success: 3 XP
- Save iButton: 3 XP
- Emulate iButton: 2 XP
- Manual Add: 2 XP

### •BadUSB

- Play Script: 3 XP

### •U2F

- Authorize success: 3 XP

# 0x02 – News About Flipper



Polícia de SP prende quadrilha que clonava controles remotos de garagens para invadir casas

Fonte: [https://www.youtube.com/watch?v=UYN\\_05h0PY0](https://www.youtube.com/watch?v=UYN_05h0PY0)



Fonte:

<https://www.joom.com/en/search/q.flipper>

Prezado(a)

O requerimento [REDACTED] foi indeferido em 23/01/2023.

A área de certificação da Anatel informa que o equipamento denominado FLIPPER ZERO tem sido utilizado no país por usuários mal intencionados na facilitação de crime ou contravenção penal e, conforme previsto no item II do Art. 60 do Regulamento de Avaliação da Conformidade e de Homologação de Produtos para Telecomunicações (anexo à [Resolução nº 715, de 23 de outubro de 2019](#)), a Anatel tem indeferido todos os requerimentos de homologação para o produto em questão, no intuito de colaborar na proteção dos cidadãos brasileiros contra ações criminosas.

A sua encomenda provavelmente será liberada para os Correios com a sugestão de devolução ao remetente.

Atenciosamente,

Fiscalização Federal – Anatel/PR

Agência Nacional de Telecomunicações – Anatel

Av. Vicente Machado, 720 - CEP 80420-011 – Curitiba/PR



## 0x02 – News About Flipper



### ANATEL ESTA BLOQUEANDO ENTREGA DE FLIPPER ZERO NO BRASIL

by Samir News - sábado, janeiro 07, 2023 2 Comentários



Fonte:

<https://www.samirnews.com/2023/01/anatel-esta-bloqueando-entrega-de.html?m=1>

### Meu Flipper foi fiscalizado pela ANATEL, e agora?



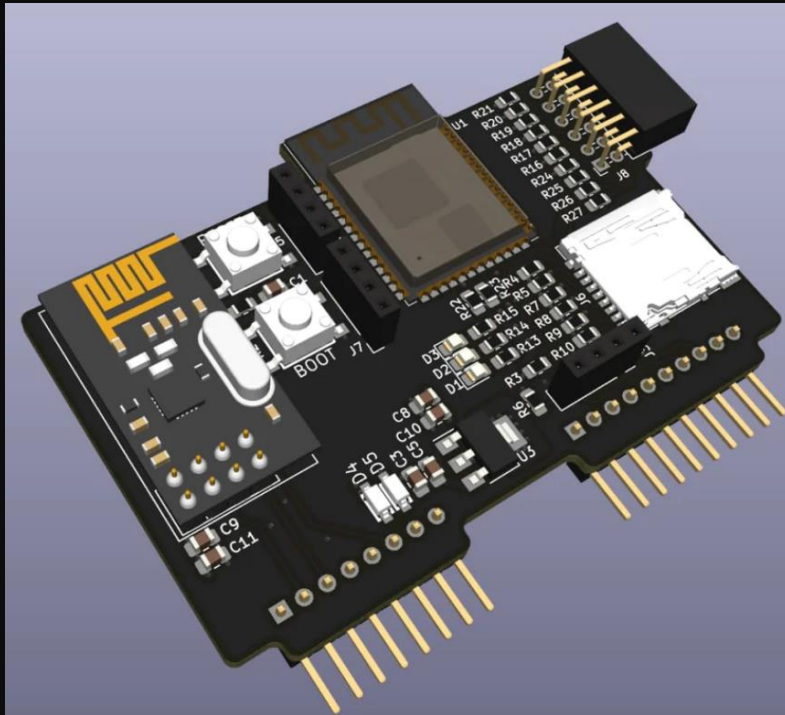
Fonte: [https://medium.com/@m4rxhs\\_cyber/meu-flipper-foi-fiscalizado-pela-anatel-e-agora-dd53fe3f6b0f](https://medium.com/@m4rxhs_cyber/meu-flipper-foi-fiscalizado-pela-anatel-e-agora-dd53fe3f6b0f)



## 0x02 - News About Flipper



### Flipper Zero Multi Expansion Board



<https://shop.tesmus.io/products/flipper-zero-multi-expansion-board>

### Aumento do Preço Flipper Zero no BR



Novo

Flipper Zero Com Placa Wifi

R\$ 7.699

em 10x R\$ 769<sup>90</sup> sem juros

[Ver os meios de pagamento](#)

[Chegará grátis entre os dias 3 e 8 fev.](#)

Você pode tê-lo entre segunda-feira e quinta-feira 2 de fevereiro por R\$ 23 R\$ 59,59

[Ver mais formas de entrega](#)

Cor: Branco

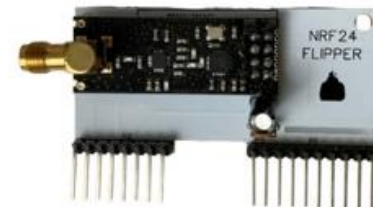
Estoque disponível

Quantidade: 1 unidade (3 disponíveis)

### Flipper Módulo For Mouse Jack





Módulo Nrf24I01 Nrf24 Sniffer Para Flipper Zero Com Antena


1/3





# 0x02 - News About Flipper



106**announcements**

25 mensagens novas desde 9:09 AM 

**ClaraCrazy | No support in DMs**  16/01/2023 05:08  
**@here**  
**Roguemaster is now spreading spyware with his firmware**  
  
<https://cloud.cynthialabs.net/s/N34N9eacLf2gdxe/preview>  
<https://cloud.cynthialabs.net/s/wi6Aw3XiY3oS6RL/preview>  
  
TL;DR:  
- Roguemaster has added a new part of code that, as long as you got bluetooth enabled, will make your Flipper behave like an airtag. Great idea.. however its not your airtag. Its Roguemasters airtag. Every time an iphone is within bluetooth range, your flipper will tell the iphone "hey I'm an airtag", the iphone will tell the icloud server "hey, im in london, randomstreet 37" and the icloud server will tell the airtag owner "hey, your thingy is right there"..  
  
Multiple Users have already noticed that, see screenshots below. Furthermore, I'd recommend reporting this to github. Wether this was an honest mistake (which I doubt) or an actual attempt of spying on users, you have to be held

Siga para receber atualizações deste canal no seu próprio servidor.  

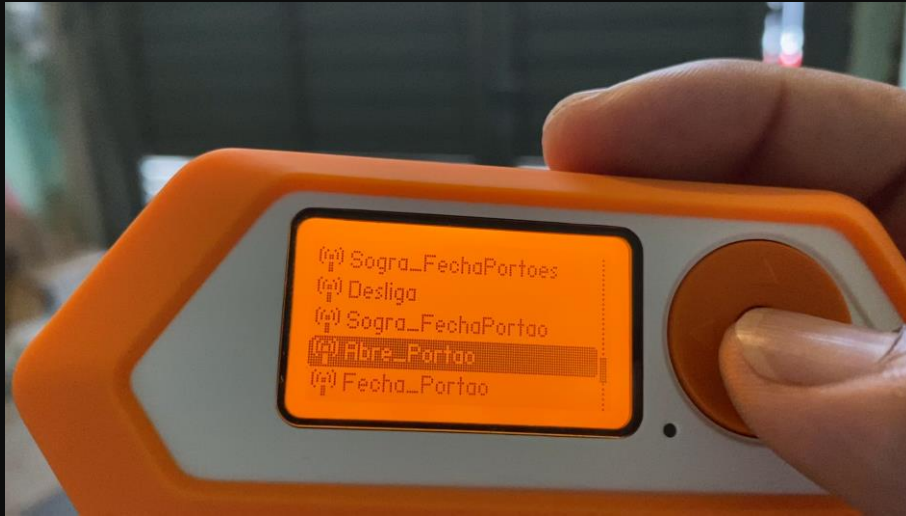
Seguir

## Firmware Roguemaster (With Spyware Firmware)

## 0x03 - Demos



Qflipper/WebUpater



Sub-GHz - Portão

Sub-GHz - Portão





Sub-GHz - Car  
(Learning Code)





Sub-GHz - Ventilador  
Arno Vx10





## NFC - Mifare Classic





NFC - xNT NFC Tag [NTAG216]

## 0x03 - Demos



### NFC – Card

Emulation on real payments not working (Brazil)

```
▼ 3 applications/main/nfc/scenes/nfc_scene_saved_menu.c
↑ 3 @@ -20,8 +20,7 @@ void nfc_scene_saved_menu_on_enter(void* context) {
20 20     Submenu* submenu = nfc->submenu;
21 21
22 22     if(nfc->dev->format == NfcDeviceSaveFormatUid ||
23 -    nfc->dev->format == NfcDeviceSaveFormatMifareDesfire ||
24 -    nfc->dev->format == NfcDeviceSaveFormatBankCard) {
23 +    nfc->dev->format == NfcDeviceSaveFormatMifareDesfire) {
25 24     submenu_add_item(
26 25         submenu,
27 26         "Emulate UID",
↑ 3
```

Fonte: <https://github.com/flipperdevices/flipperzero-firmware/commit/01f7a3e5b52fa1842bb3117d7adddf059807c9ef>

Changelog 0.68.1 Fonte: <https://github.com/flipperdevices/flipperzero-firmware/releases/tag/0.68.1>

## 0x03 - Demos



U2F - 2Factory Authentication  
on Gmail account



DuckScript  
(Payloads)

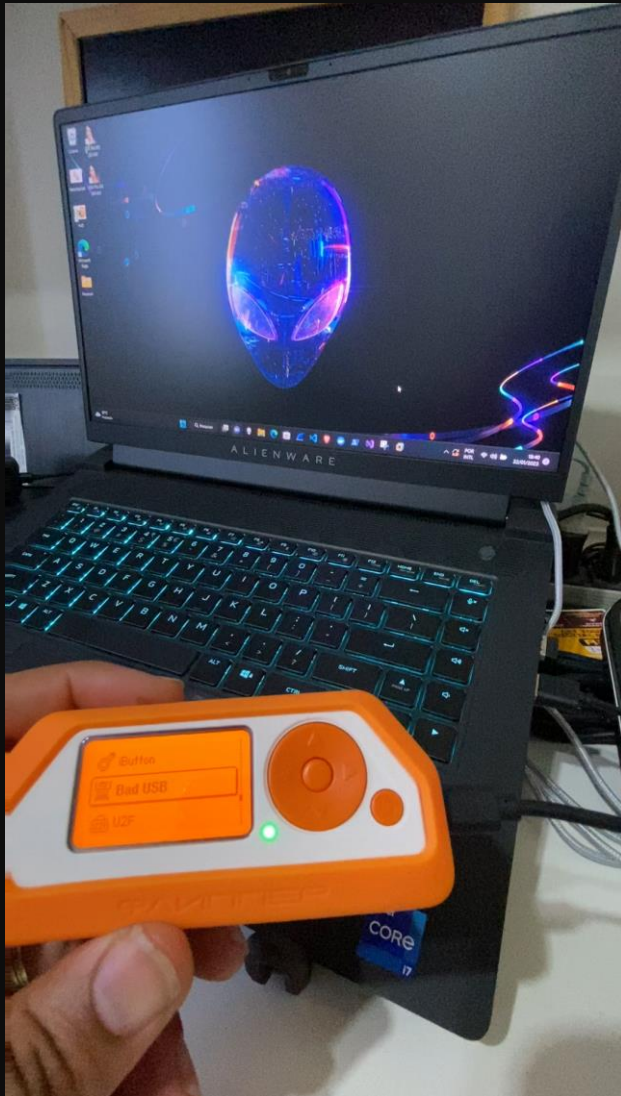


# 0x03 - Demos

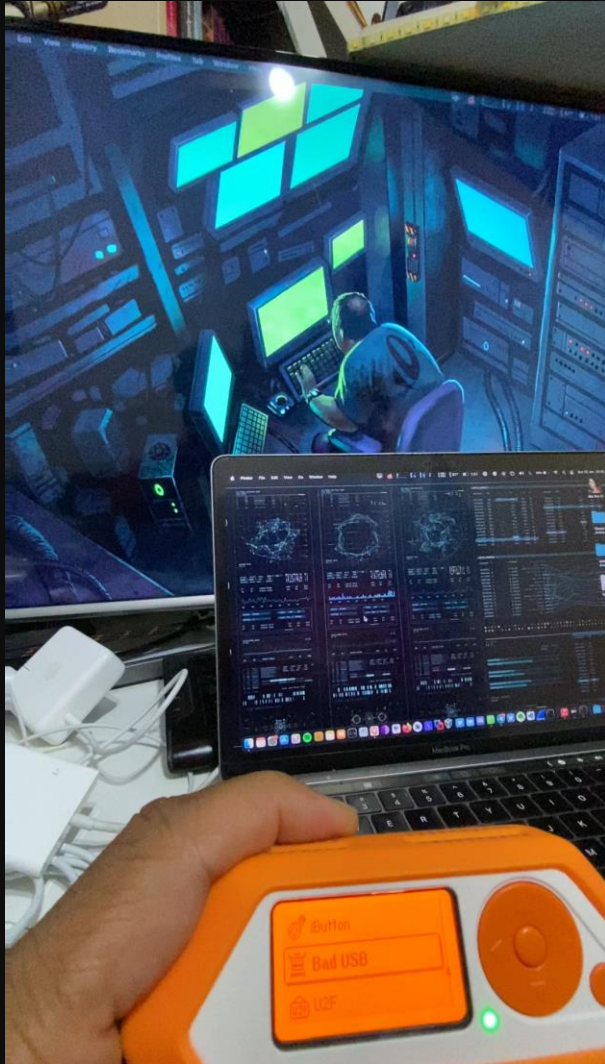


BadUSB – macOS RevShell





BadUSB – Open URL (Browser) Windows 11



BadUSB – Open URL (Browser) macOS



BadUSB – Android Send msg Whatsapp



BadUSB - Linux TermBomb





GPIO – ESP32 (Marauder) – Death Wifi Network



## GPIO – NRF24 – Mouse Jack Attack

Target Logitech m170



## 0x04 - Conclusion



Device  
Compacto  
porém  
completo e  
expansível

Simulações  
de Red  
Team

Produto  
virou  
febre

Anatel e órgãos  
reguladores  
proibindo a  
homologação e  
uso do Flipper.

Open-Source

ML com  
anúncios de  
até 8mil  
reais.

# 0x04 - Conclusion



## Kali Linux Integration

A promotional image for the Flipper One device. The device is a small, black, rectangular unit with a small screen displaying a cartoon duck and the word 'FLIPPER'. It has a large orange button and a smaller orange button. The device is surrounded by various tools and components, including a soldering iron, a blue USB drive, a SIM card, a small circuit board, and a yellow and black striped banner that reads 'UNDER DEVELOPMENT final look and features may change'.

# Flipper One

Multi-tool Device for Hackers

Join the development

Based on i.MX6 SoC

Kali Linux full support

Open Source Software and Hardware

Community-driven development Voting for features

Fonte: <https://forum.flipperzero.one/t/kali-linux-integration/2452>

## 0x05 - Reference



### Projeto

<https://flipperzero.one>

### Comprar Flipper

<https://www.joom.com/en/search/q.flipper>

### Firmware Unleashed

<https://github.com/DarkFlippers/unleashed-firmware>

### Extra

<https://github.com/UberGuidoZ/Flipper>

<https://github.com/djsime1/awesome-flipperzero>

### Mouse Jack

<https://www.mousejack.com>

Thanks a Lot

Any Questions ?

