# RF Hacking with Flipper Zero

# Whoami

## Antony Mutiga

- N00b Pentester
- Everything Sports
- @AntonyMutiga
- Blog

# Agenda

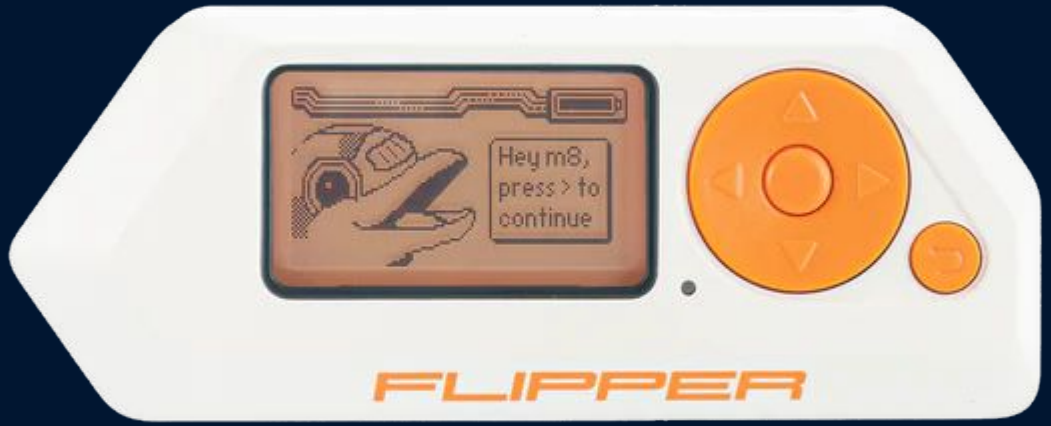
- What is RF Hacking?
- What is a Flipper Zero?
- RF landscape in Kenya
- CA Guidelines
- Demo
- References

# What is RF Hacking?

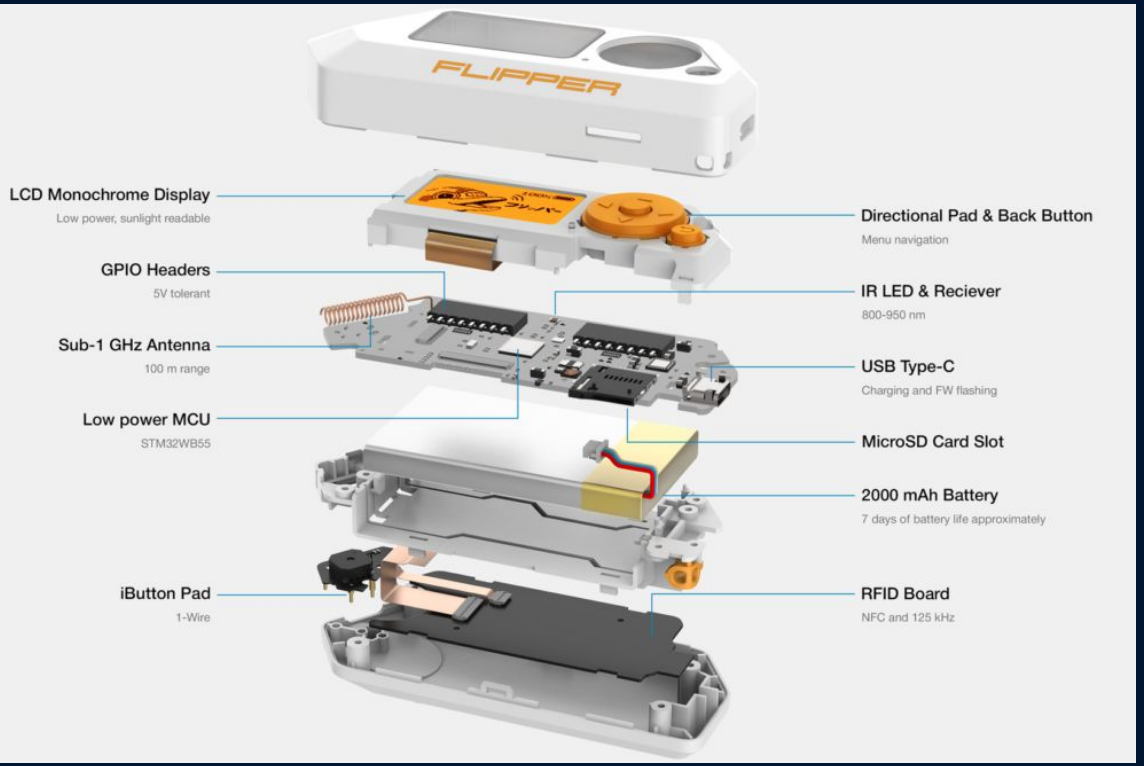
- Radio Frequency (RF) Hacking is the process of being able to capture, decode, replay and hack radio signals.

# What is a Flipper Zero?

- Flipper Zero is a portable multi-tool for pentesters and hardware geeks in a toy-like body. It loves to explore the digital world around: radio protocols, access control systems, hardware, and more.



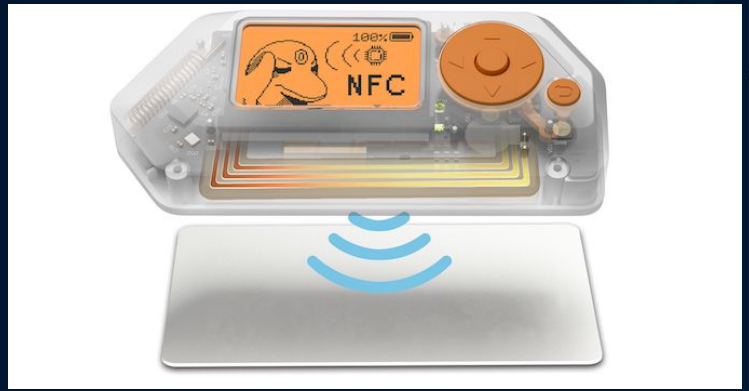
# What’s inside a Flipper Zero



# What can the Flipper Zero do?

- **A Sub 1 GHz antenna** - The Flipper Zero can scan, capture and playback certain radio frequencies. It can mostly open devices like car key fobs, IoT sensors, garage doors, parking gates etc.

- **RFID Board (which also reads NFC)** - RFID is an increasingly common technology that allows for small amounts of data to be transmitted from a non-powered device, like an access card or a product tag, to a reader, such as a door lock or a register. The Flipper Zero can read RFID values, save, and replay them.



# What can the Flipper Zero do?

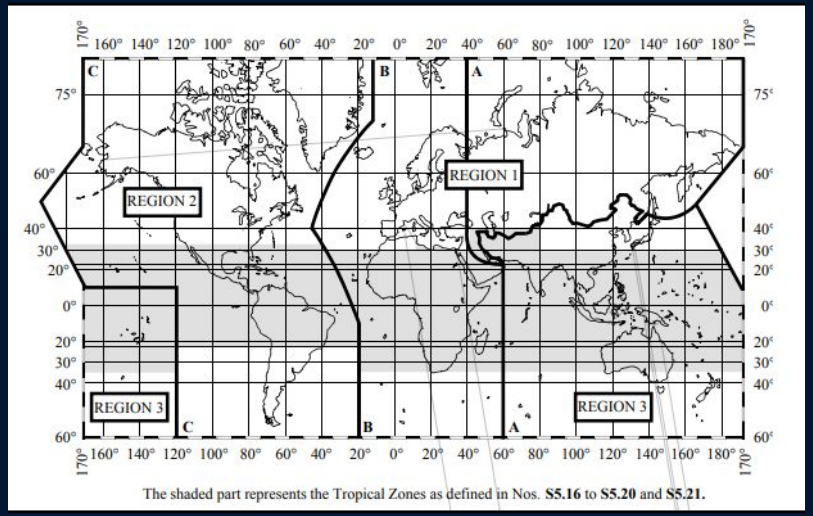
- **IR LED & Receiver** - The Flipper contains an infrared transceiver and it can help one control TVs, ACs, Audio Systems and other devices that use infrared signals. You can also save a specific remote signal and you can then turn your Flipper into a remote.


- **GPIO Headers** - The Flipper has a standard 2.54 mm GPIO header on the side, connected to the MCU pins. There are SPI, I2C, UART and other peripheral offered by our STM32. These pins can be used to connect 3rd party devices via industrial protocols. GPIO has 3.3V and 5V pins which allow to power connected module directly.

# Flipper Sub-GHz hardware

Flipper Zero has a built-in sub-1 GHz module based on a **CC1101** chip and a radio antenna. 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.

# RF landscape in Kenya




- Kenya is located in Region 1.
- Allowed to transmit: **433.05 - 434.79** MHz; **868.15 - 868.55** MHz.
- CA is the regulatory authority for the communications sector in Kenya.

Source: https://www.ca.go.ke/wp-content/uploads/2021/03/National-Table-of-Frequency-Allocations-2020.pdf

# Communications Authority (CA) Guidelines

CA classifies a device like the Flipper Zero as a **Short Range Radio Device** (**SRDs**).

**Short Range Radio Devices (SRDs)** are transmitters or receivers or both that generate and use radio frequencies.

# Communications Authority (CA) Guidelines

Below is a list of frequencies listed by CA that operate within the Flipper Zero's range including their power, spectrum access, modulation and standard:

| | Frequency Band | Power / Magnetic Field | Spectrum access and mitigation | Modulation / max. bandwidth | Relevant Standard | Notes |
|---|---|---|---|---|---|---|
| a. | 433.05 - 434.79 MHz | 1 mW e.r.p. | 100% duty cycle.<br>10 mW e.r.p. 100% duty cycle | Up to 25 KHz Channel spacing | EN 300 220; EN 301 489 | |
| b. | 868.0 - 868.6 MHz | 25mW e.r.p. | ≤1% duty cycle or LBT+AFA | Non Specified | EN 300 220; EN 301 489; EN 60950 | |
| c. | 868.7 - 869.2 MHz | 25mW e.r.p. | ≤1% duty cycle or LBT+AFA | | EN 300 220; EN 301 489<br>EN 60950 | |
| d. | 865.0 - 868.0 MHz | 500mW e.r.p.<br>Transmissions only permitted within 4 sub-bands | Adaptive Power Control (APC) required.<br>Bandwidth: ≤ 200 kHz Duty | | EN 300 220; EN 301 489<br>EN 60950<br>Directive 2014/53/EU | Restricted to 4 channels only with Adaptive Power Control (APC) required. |
| | | 865.6 - 865.8 MHz;<br>866,2 - 866.4 MHz;<br>866,8 - 867.0 MHz;<br>867.4 - 867.6 MHz. | cycle: ≤ 10 % for network access points Duty cycle ≤ 2,5 % otherwise | | | |
| e. | 869.4-869.65 MHz | 500mW e.r.p. | ≤10% duty cycle or LBT+AFA | | EN 300 220; EN 301 489<br>EN 60950 | |
| f. | 869.7- 870 MHz | 5mW e.r.p. | No Requirement | | EN 300 220; EN 301 489<br>EN 6095 | |
| g. | 869.7- 870 MHz | 25mW e.r.p. | ≤10% duty cycle or LBT+AFA | | EN 300 220; EN 301 489<br>EN 60950 | |
| p. | 402-405 MHz | 25 µW e.r.p. | LBT No duty cycle, Otherwise ≤ 1%. | 25 kHz Channel spacing. | EN 301 839; EN 301 489<br>EN 60950; EN 300 220 | Medical implants MICS |
| q. | 446-446.1 MHz includes the following 8 channels.<br>446.00625;<br>446.01875;<br>446.03125;<br>446.04375;<br>446.05625;<br>446.08125;<br>446.09125;<br>446.09375 | 500mW e.r.p. | | 12.5 kHz channel spacing | EN 300 296; EN 301 489<br>EN 60950 | Family Radio<br>Two Way Communications Systems<br>Citizen Band |

Source: https://www.ca.go.ke/wp-content/uploads/2022/07/Guidelines-on-the-Use-of-Radiofrequency-Spectrum-by-Short-Range-Devices-2022.pdf

# CA Guidelines - Allocations

Below is a list of frequencies allocations by the CA within the Flipper's range:

**290 – 387 MHz**

| FREQUENCY BAND IN MHz | ALLOCATION TO SERVICES | REMARKS |
|---|---|---|
| 290 - 328.6 | FIXED *K51 K88* | Fixed links |
| 328.6 – 335.4 | AERONAUTICAL RADIONAVIGATION *K90* | Instrument landing systems |
| 335.4 – 345 | FIXED K88 | Fixed Wireless Access New fixed links prohibited |
| 345 - 360 | FIXED *K88* | Fixed Wireless Access New fixed links prohibited |
| 360 - 377 | FIXED *K88* | Fixed Wireless Access New fixed links prohibited |
| 377 - 380 | FIXED MOBILE *K88* | Fixed Wireless Access (TDD) |
| 380 - 387 | FIXED *K88* | Fixed links Fixed Wireless Access |

Source: https://www.ca.go.ke/wp-content/uploads/2021/03/National-Table-of-Frequency-Allocations-2020.pdf

# CA Guidelines - Allocations

**387 – 406.0 MHz**

| FREQUENCY BAND IN MHz | ALLOCATION TO SERVICES | REMARKS |
|---|---|---|
| 387 - 390 | FIXED MOBILE *K88* | Public safety & emergency network |
| 390 - 397 | FIXED *K91 K88* | Public safety & emergency network |
| 397 – 399.9 | FIXED MOBILE *K88* | Public safety and emergency network |
| 399.9 – 400.05 | MOBILE SATELLITE (Earth – space) *K78, K79,K91A* | Little LEOs, earth stations in the mobile-satellite service |
| | RADIONAVIGATION SATELLITE *K80 K81* | Radionavigation satellite |
| 400.05 - 400.15 | STANDARD FREQUENCY & TIME SIGNALS *K92* | Standard time and frequency signals reception (400.1 MHz) |
| 400.15 – 406 | METEOROLOGICAL AIDS METEOROLOGICAL SATELLITE (space-to-Earth) MOBILE-SATELLITE (space-to-Earth)<br>SPACE RESEARCH (space-to-Earth)<br>EARTH EXPLORATION-SATELLITE (Earth-to-space)<br>Space operation (space-to-Earth) | Meteorological aids<br>Meteorological satellite<br>Mobile satellite<br>Space operation |

**406.0 – 430 MHz**

| FREQUENCY BAND (MHz) | ALLOCATION TO SERVICES | REMARKS |
|---|---|---|
| 406.0 – 406.1 | MOBILE-SATELLITE (Earth-space) *K93* | Low power EPIRBs for Search and Rescue |
| 406.1 – 410 | FIXED *K51* | Fixed links-Government use |
| | MOBILE except aeronautical mobile K51 | Government use |
| | RADIO ASTRONOMY *K93A* | Radio Astronomy |
| 410 - 430 | MOBILE except aeronautical mobile *K94* | Land Mobile (Trunked Radio) |
| | FIXED K94 | Fixed New fixed links prohibited |

**430 – 455 MHz**

| FREQUENCY BAND (MHz) | ALLOCATION TO SERVICES | REMARKS |
|---|---|---|
| 430-450 | MOBILE K95 K96 | Land Mobile Low power private radio (PMR 446) |
| | FIXED K95 | Fixed |
| | *Amateur K96* | Amateur User licence required |
| 450 – 470 | MOBILE *K97* | Band identified for IMT Resolution 224 (Rev.WRC-19) |
| | FIXED *K98* | Fixed links, FWA onsite paging, wide area paging, land mobile, radio alarms prohibited |

**470 – 694 MHz**

| FREQUENCY BAND (MHz) | ALLOCATION TO SERVICES | REMARKS |
|---|---|---|
| 470 – 694 | BROADCASTING*K62 K100* | UHF digital terrestrial Television broadcasting (Bands IV & V) Channels 36-48 |
| | Mobile *K99* | Land mobile – Limited to applications ancillary to broadcasting and programme making |

**694 – 960 MHz**

| FREQUENCY BAND (MHz) | ALLOCATION TO SERVICES | REMARKS |
|---|---|---|
| 703 - 862 | MOBILE *K101* | Mobile Band identified for IMT services |
| 862 - 960 | FIXED *K101* | Fixed wireless access networks |
| | MOBILE *K102, K103* | Public cellular Mobile networks |

**960 - 1350 MHz**

| FREQUENCY BAND (MHz) | ALLOCATION TO SERVICES | REMARKS |
|---|---|---|
| 960 – 1164 | AERONAUTICAL RADIONAVIGATION *K105* | Distance measuring equipment |
| | AERONAUTICAL MOBILE (R) *K104, K104A* | Aeronautical Mobile<br>Aeronautical mobile-satellite (R) service (E-S) |

Source: https://www.ca.go.ke/wp-content/uploads/2021/03/National-Table-of-Frequency-Allocations-2020.pdf

# CA Guidelines - Allocations

**LIST OF ACCESS FREQUENCIES ASSIGNED TO OPERATORS**

**A. MOBILE WIRELESS ACCESS**

| Frequency Band | Amount of Spectrum | Assigned Operator |
|---|---|---|
| 800 MHz | 5MHz paired | Telkom Kenya Limited<br>P.O. Box 30301-00100<br>NAIROBI |
| 900 MHz | 10MHz paired | Safaricom Limited<br>P.O. Box 46350-00100<br>NAIROBI |
| 900 MHz | 10MHz paired | Celtel Kenya Limited<br>P.O. Box 73146-00200<br>NAIROBI |
| 900MHz | 7.5MHz paired | Telkom Kenya Limited<br>P.O. Box 30301-00100<br>NAIROBI |
| 900MHz | 7.5MHz paired | Essar Telecom Kenya Limited<br>P.O. Box 45742-00100<br>NAIROBI |

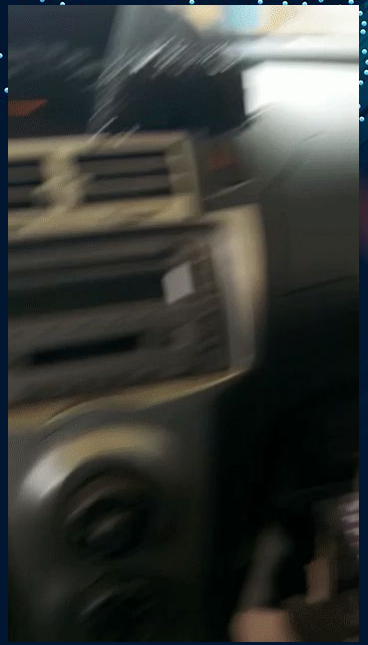
# Limitations of the Flipper

- Doesn’t have support for car key fobs that use rolling codes.
- Can’t receive and transmit signals over 1GHz.
- It is not a SDR (Software Defined Radio)

# Demo

# Conclusion

- This is a great device for light pentesting!
- The community is great and can’t wait to see how far the device will improve as more people join the community.
- When using the Flipper please use it RESPONSIBLY!



# Resources

- https://www.kickstarter.com/projects/flipper-devices/flipper-zero-tamagochi-for-hackers
- https://www.ca.go.ke/wp-content/uploads/2021/03/National-Table-of-Frequency-Allocations-2020.pdf
- https://www.ca.go.ke/wp-content/uploads/2022/07/Guidelines-on-the-Use-of-Radiofrequency-Spectrum-by-Short-Range-Devices-2022.pdf
- https://cyberprosolutions.net/flipper-zero-overview/

# THANKS!

Do you have any questions?
antony@cyberprosolutions.net
+254733640066
https://cyberprosolutions.net/