easy Former
La formation à 360°

FLIPPER ZERO

Sous-titre (description)

Référence : TYPE-TECHNO-MODULE-1999

Auteur :
Wilfried RAVISSOT
Adrien MUHLHEIM
Leo COLIN

Destinataires :
Formateurs
Apprenants

Date de dernière modification : 27/04/23

Version : 1.0

Remerciements

EasyFormer est une organisation dont l'un des objectifs est de mutualiser les efforts de tous afin d'améliorer la qualité de la formation et d'aider les centres à proposer un contenu plus ciblé et exhaustif.

Nous tenons à remercier chaleureusement tous les généreux contributeurs bénévoles ou non (rédacteurs, formateurs, stagiaires, apprenants ou autres) qui ont participé à la rédaction, l'amélioration et la correction de nos supports de cours et de travaux pratiques.

Devenez contributeur

Pour contribuer à l'effort collectif et aider les mécanismes de formation nationaux vous pouvez :

- rédiger des paragraphes,
- proposer des améliorations à nos supports,
- signaler les coquilles orthographiques ou grammaticales,
- proposer des compléments (rédigés ou non),
- rectifier ou mettre à jour des informations techniques.

Et envoyer votre travail à **doc@easyformer.fr**

Vous trouverez ci-dessous une liste non exhaustive (et qui ne respecte pas d'ordre précis) de contributeurs qui ont participé à la rédaction des documents EasyFormer :
https://cloud.easyformer.fr/index.php/s/contributeurs

REMERCIEMENTS 2
DEVENEZ CONTRIBUTEUR 2

1 INTRODUCTION 4

1.1 PRESENTATION 4
1.2 LES CAPACITES DU FLIPPER 4
1.3 CARACTERISTIQUES 5
1.4 OU L'ACHETER ? 5

2 UTILISATION BASIC 6

2.1 POWER 6
2.1.1 Démarrage et redémarrage de l'appareil 6
2.1.2 Eteindre l'appareil 7
2.2 MISE A JOUR 8
2.2.1 Téléphone APP 8
Partie 1 : Installation et synchronisation 8
Partie 2 : Mise à jour 9
2.2.2 Ordinateur APP 10

3 UTILISATION DES LOGICIELS D'HACKING 11

3.1 NFC 11
3.1.1 Lire un badge 12
3.1.2 Débloquer un badge comportant un mot de passe 13
3.2 RFID 15
3.2.1 Lire un badge 15
3.3 SUB-GHZ 16
3.3.1 Analyser sa fréquence 16
3.3.1 Lire une fréquence 16
3.3.2 Lire une fréquence Brute 18
3.4 INFRAROUGE 19
3.4.1 Universal Remotes 20
3.4.2 Ajout d'un signal infrarouge 21
3.5 BAD USB 22
3.5.1 Utilisation de Bad USB 23
3.6 IBUTTON 24

1 Introduction

La majorité des images du Flipper ZERO présente dans ce document son prise depuis le site officiel : https://flipperzero.one/

1.1 Présentation

Ce cours a pour objectif de vous faire comprendre les principaux concepts du Flipper ZERO et vous fournir des connaissances basiques en la matière.

Le Flipper ZERO est né d'un crowdfunding sur KICKSTARTER rassemblant 4 882784 $ en 2020.

C'est un outil portable d'hacking et est principalement destiné aux pentesters ou pour des alternative ludique et éducative.

Sa popularité est tel, qu'il est généralement en rupture de stock. Cette popularité est dû à la facilité de l'utilisation du flipper et a son aptitude à hacker des dispositifs comme certaine voiture dont des TESLA.

1.2 Les capacités du Flipper

Il dispose de la quasi-totalité du petit attirail de l'hacker.

Disposant d'une antenne inférieure à 1 GHz, du NFC, RFID, l'infrarouge, de 18 connecteurs GPIO (General Purpose Input/Output) ou encore d'une connectique iButton vous pouvez ouvrir la casi totalité des portes présente sur le marché.

Attention les normes et protection informatique évoluent très vite, mettez donc bien à jour votre Flipper ZERO pour être sûre d'avoir les derniers moyens d'hacking.

1.3 Caractéristiques

- Arm Cortex-M4 32 bits 64 MHz (puce mobile)
- Arm Cortex-M0+ 32 MHz (puce réseau)
- **Flash :** 1 024 Ko
- **SRAM :** 256 Ko
- **Ecran :** monochrome LCD 128 x 64 de 1,4 pouce
- **Joystick :** 5 boutons avec bouton retour
- **Batterie :** rechargeable de 2 000 mAh
- **Fréquences inférieures à 1 GHz :** 315 MHz, 433 MHz, 868 MHz et 915 MHz (selon les régions)
- **NFC :** 13,56 MHz
- **RFID :** 125 kHz
- Connecteur : 18 GPIO
- **Infrarouge :** gamme TX/RX : 800-950 nm, puissance TX : 300 mW
- **Support :** iButton 1— Wire (compatible Dallas DS1990A/CYFRAL)
- **Port USB :** 2.0 type-C

1.4 Ou l'acheter ?

Le flipper ZERO est achetable soit via le site officiel soit via des revendeurs comme LAB401, pour une maudite somme de 169€.

Les modules complémentaires officiel comme le module de wifi coute environ 40€.

Site officiel Flipper ZERO : https://flipperzero.one/

Revendeur LAB401 : https://lab401.com/fr

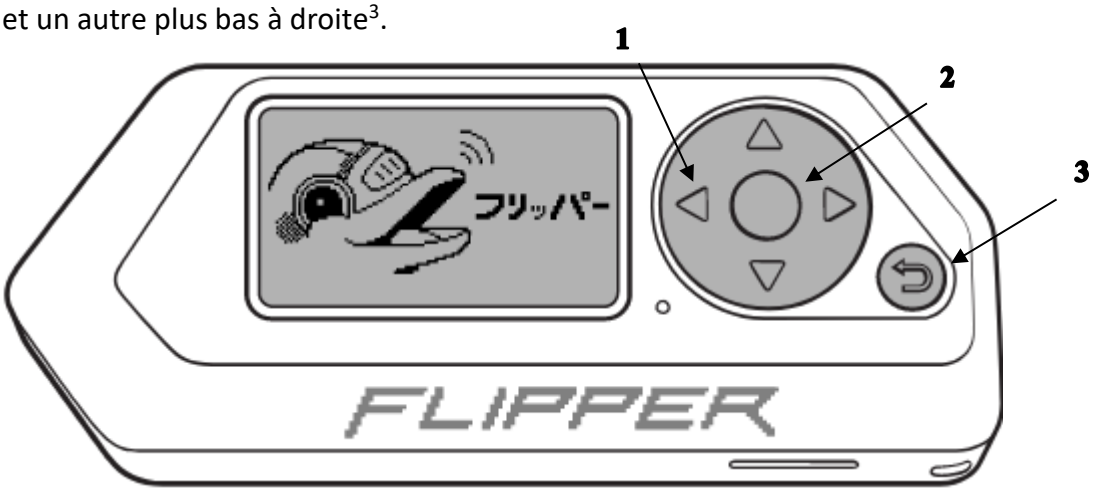
2 Utilisation Basic

Nous recommandons fortement d'aller sur la documentation officielle du Flipper, en plus d'avoir une documentation très bien faite, elle risque d'être à jour contrairement à celle-ci.

2.1 Power

2.1.1 Démarrage et redémarrage de l'appareil

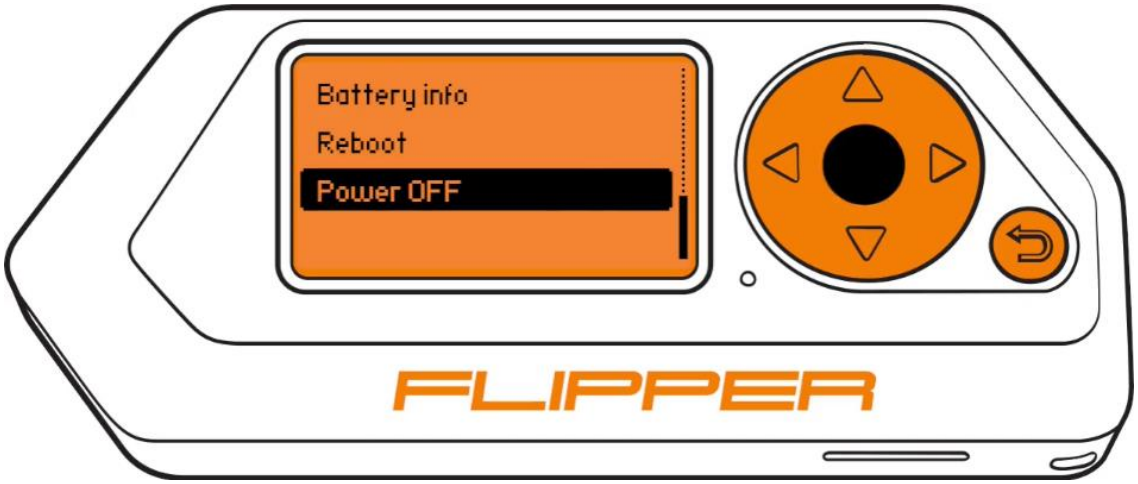
Le Flipper ZERO se contrôle avec des flèches directionnelles[1] et 2 boutons, un entre les flèches[2] et un autre plus bas à droite[3].



Vous pouvez l'**allumer** avec le bouton en bas à droite[3] et le **redémarrer** avec la flèche directionnel gauche[1] et le bouton en bas à droite[3].

2.1.2 Eteindre l'appareil

Pour l'arrêter il faut vous diriger dans **Settings → Power → Power OFF**



2.2 Mise à jour et utilisation des APPS

La mise à jour se fait soit via l'application du flipper installé soit sur votre téléphone soit sur un ordinateur. Une carte SD de 4 Go minimum est obligatoire.

Plus d'information via le lien suivant : https://docs.flipperzero.one/basics/firmware-update

L'utilisation des applications est assez simple je vous conseille fortement de fouiller, j'ai d'ailleurs trouvé sur l'application sur telle la possibilité de prendre la main à distance du flipper avec une option expérimentale à activer.

2.2.1 Téléphone APP

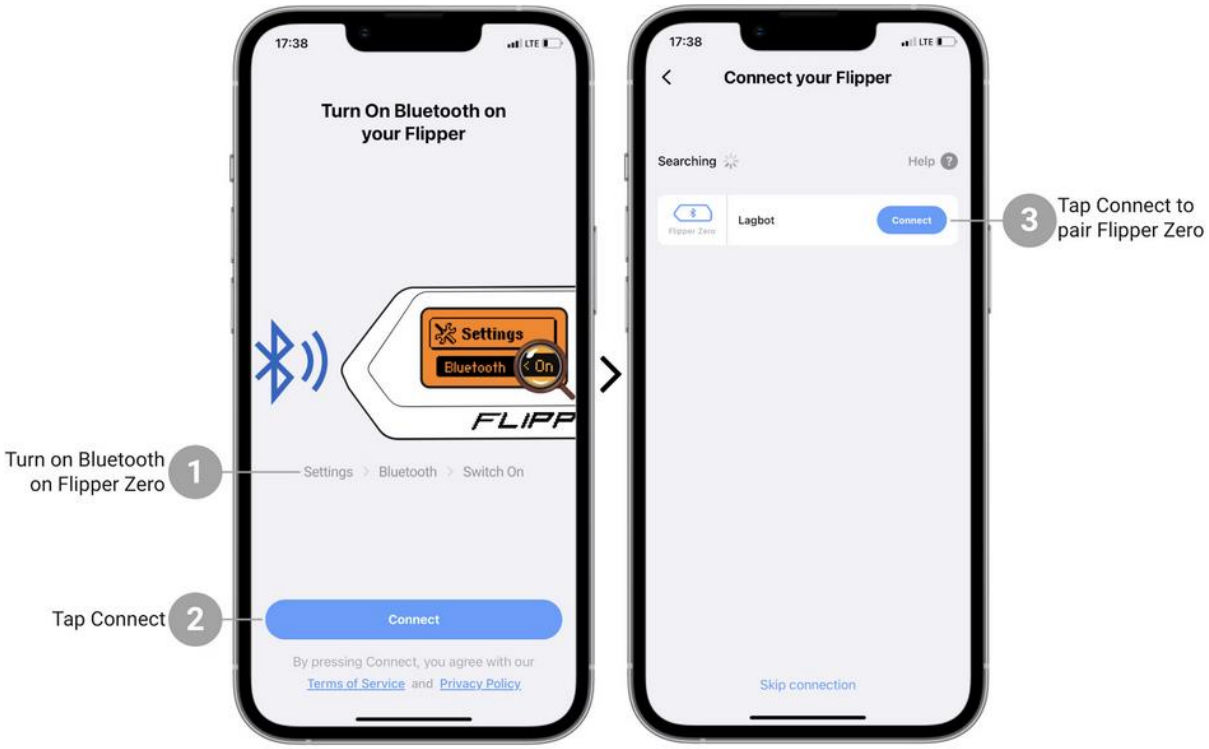
Partie 1 : Installation et synchronisation

Sur téléphone, télécharger **Flipper Mobile App** depuis l'APP Store ou le Play Store.

Pendant le téléchargement vous pouvez commencer à démarrer le Bluetooth du Flipper dans **Settings → Bluetooth**.

Attention le Bluetooth est obligatoire pour l'utilisation de l'application depuis votre téléphone.

Après l'installation ouvrée l'application et suivez les consignes.

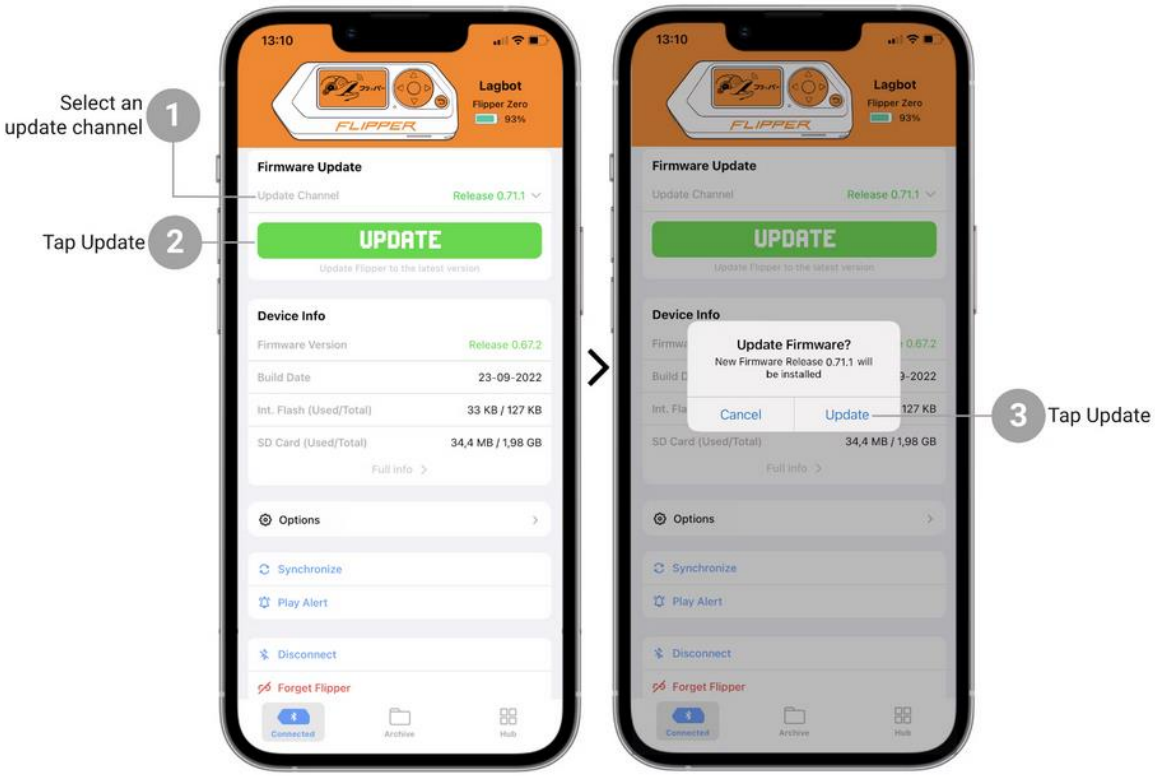


En bas à gauche vous pouvez voir l'état de la synchronisation entre votre téléphone et le Flipper. Nous vous recommandons de synchroniser si cela fait plusieurs minutes que vous n'avais pas utiliser le flipper pour l'application.

Partie 2 : Mise à jour

La mise à jour se fait via le bouton en plein milieu **UPDATE**, on vous demandera une confirmation → **UPDATE**

Puis suivez les indications.



 Date : 27/04/23

2.2.2 Ordinateur APP

Pour commencer télécharger le logiciel pour Windows ici

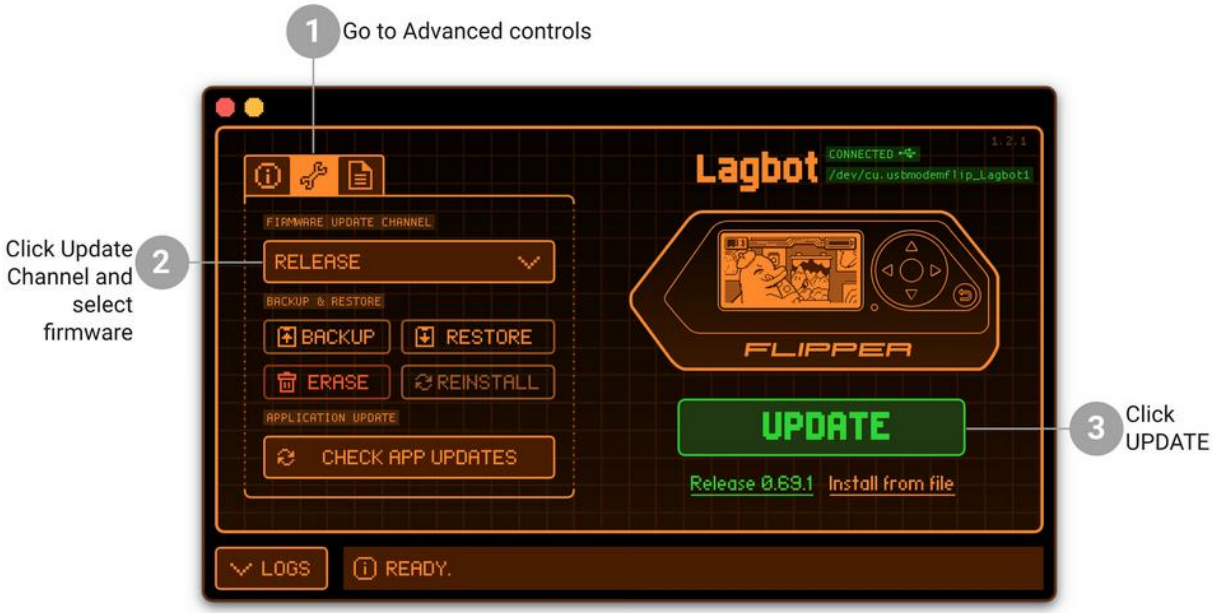
Si le lien ne fonctionne pas ou que vous utilise un MAC, veuillez-vous reporter via la documentation officielle le lien est fourni plus tôt dans la documentation.

Une fois télécharger et installé, démarrer le logiciel et connecter votre flipper avec le cordon USB-C vers USB-A a votre ordinateur.

Si tout est dans le vert, le logiciel reconnait directement le flipper et vous aurez à droite la possibilité de le mettre à jour avec **UPDATE**.

Dans le 2ème onglet en haut à gauche vous avez la possibilité de choisir le type de version du micrologiciel ou de vérifier si une mise à jour est disponible plus bas.

Pour information vous avez dans le 3ème onglet la possibilité d'ajouter vos programme et script sur la carte SD.



A la suite, il vous suffit suivre les étapes que le flipper vous indique directement sur le logiciel ou l'équipement.

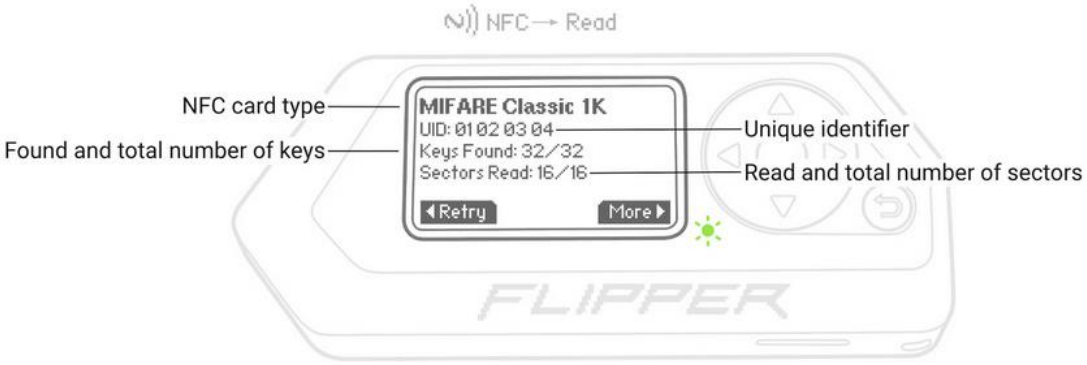
3 Utilisation des logiciels d'Hacking

3.1 NFC

NFC (Near Field Communication) est une technologie sans fil à courte portée qui permet aux dispositifs de communiquer entre eux lorsqu'ils sont à proximité l'un de l'autre, généralement à quelques centimètres.

La technologie NFC est couramment utilisée pour les paiements sans contact, où un dispositif mobile est approché d'un terminal de paiement pour effectuer une transaction. Elle est également utilisée dans d'autres applications telles que le partage de fichiers, le contrôle d'accès ou encore certain badge d'immeuble, exemple votre carte Navigo.

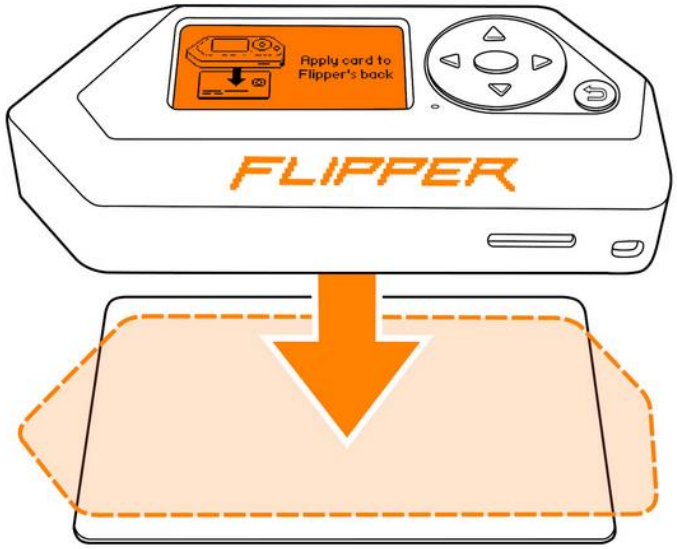
Attention la carte SD est obligatoire pour le stockage des identifiant NFC



Certaine carte ne peut être entièrement lu par Flipper, je vous recommande de lire la documentation officielle ici

3.1.1 Lire un badge

Pour lire une carte NFC, aller dans **NFC → Read** et déposez votre carte NFC en dessous du Flipper. Attendez quelques secondes le temps que le flipper lis votre badge.



A la suite vous pouvez l'émuler le sauvegarder ou voire les infos du badge en allant sur

More → Save/Emulate/Info

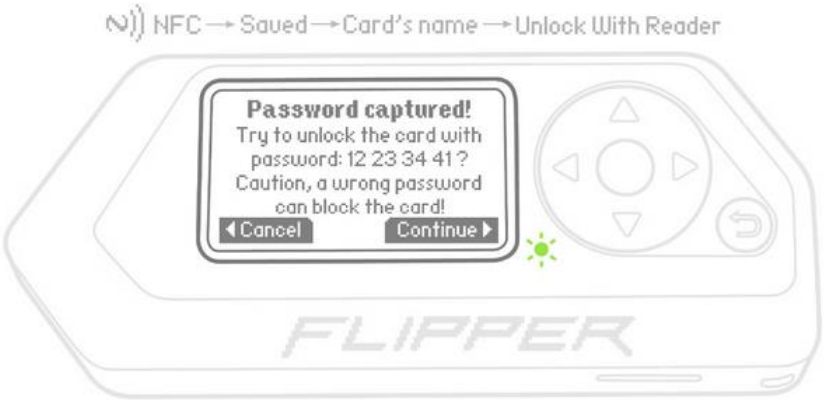
3.1.2 Débloquer un badge comportant un mot de passe

Certain badge dispose d'une protection et ne peuvent être lu sans mot de passe.

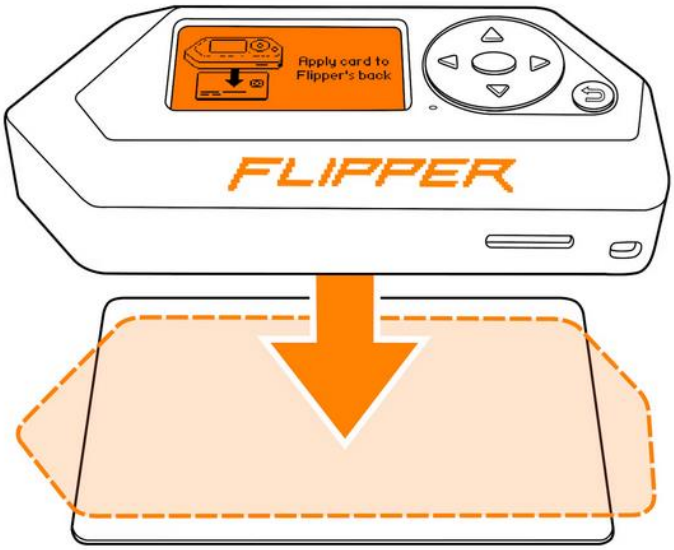
Attention cette partie doit être réaliser après avoir sauvegarder un badge sur le Flipper.

Pour cela vous devez extraire le mot de passe du lecteur, aller devant le lecteur activer l'option déverrouiller avec le lecteur dans **NFC → Saved → Card's name → Unlock With Reader** et placer le Flipper devant de lecteur plusieurs fois s'il le faut.

Lorsque le mot de passe est capturé, appuyer sur **Continue**.



Placer le badge en dessous du Flipper



Une fois déverrouiller vous pouvez sauvegarder le badge avec le mot de passe **SAVE**

3.2 RFID

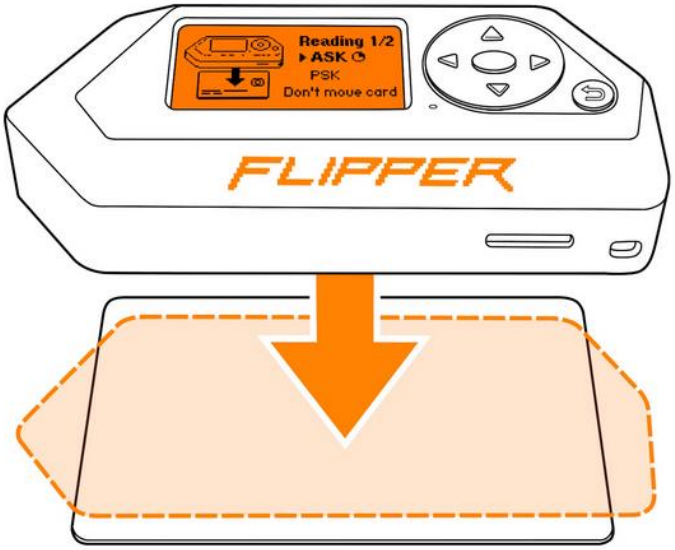
Le RFID (Radio Frequency Identification) est une technologie qui permet l'identification automatique et sans contact d'objets ou de personnes à l'aide d'ondes radio. Le système de RFID est constitué de deux éléments principaux, un badge RFID et un lecteur RFID

Certaine carte RFID ne peut être entièrement lu par Flipper, je vous recommande de lire la documentation officielle ici

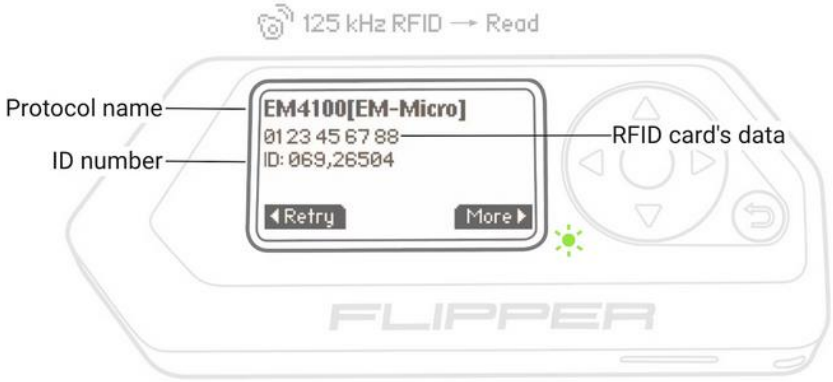
Attention la carte SD est obligatoire pour le stockage des identifiant RFID

3.2.1 Lire un badge

Pour lire un Badge aller dans **125 kHz RFID → Read** et placer votre badge en dessous du Flipper et attendez quelque seconde.



Une fois la carte lu dans **More** vous avez la possibilité de le sauvegarder, l'émuler ou de le réécrire sur un autre badge RFID.



 Date : 27/04/23

3.3 Sub-GHz

Le Sub-GHz est une fonctionnalité permettant de lire les signaux radio de moins de 1GHz.

Pour rappel en Europe les fréquences utilisées sont :

433.05 - 434.79 MHz

868.15 - 868.55 MHz

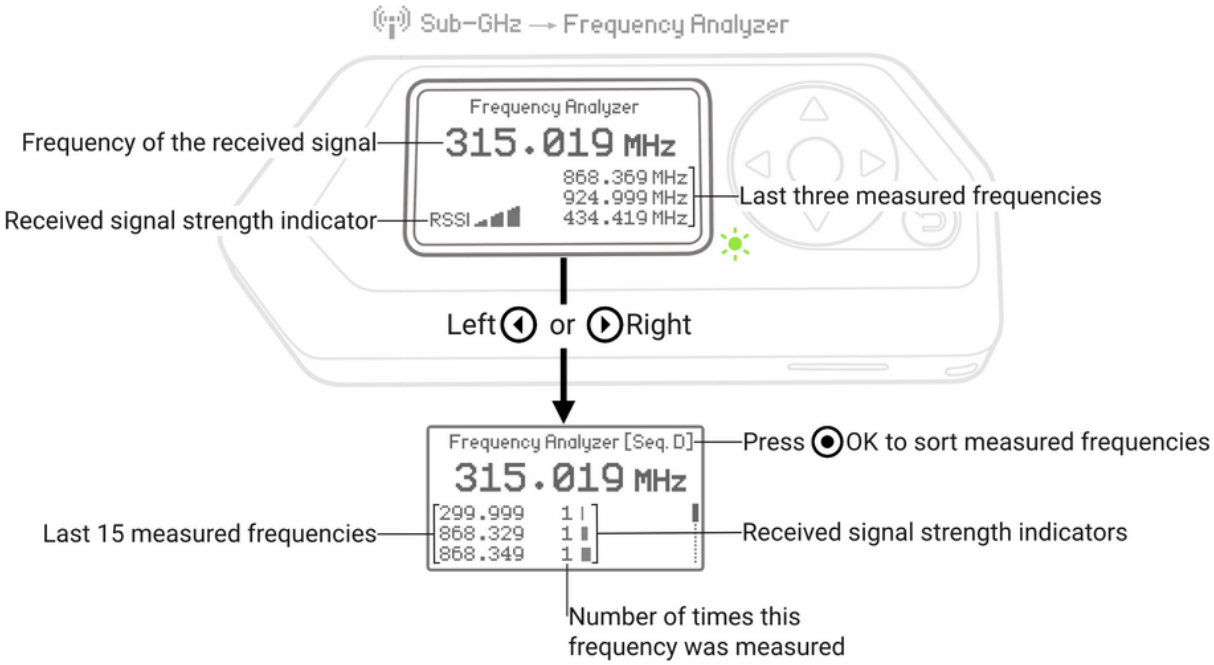
Ces fréquences son généralement utilisé pour l'ouverture des portails ou des voitures à distance.

Attention la carte SD est recommandée pour le stockage des identifiants.

3.3.1 Analyser sa fréquence

Avant de pouvoir lire un signal il vous faut connaitre sa fréquence.

Pour cela aller dans **Sub-GHz → Frequency Analyser** et utiliser votre émetteur (badge d'ouverture de garage ou voiture)

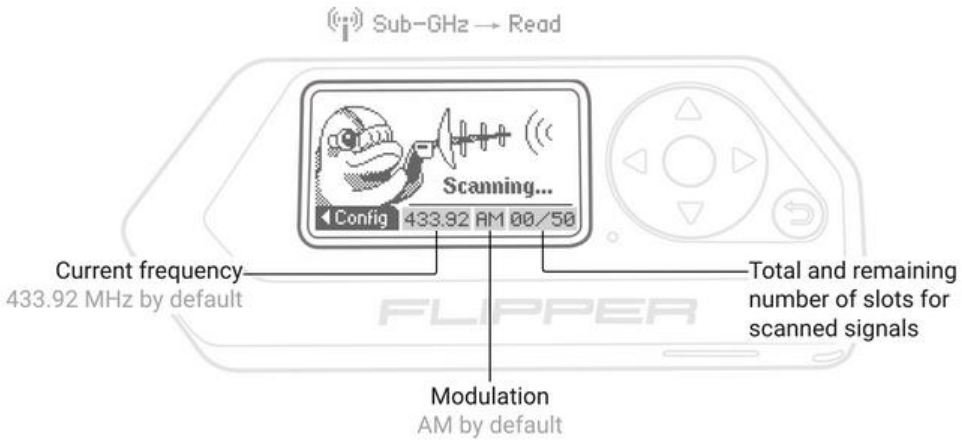


A ce moment l'analyser affiche les fréquences perçues, noter bien votre fréquence elle servira plus tard.

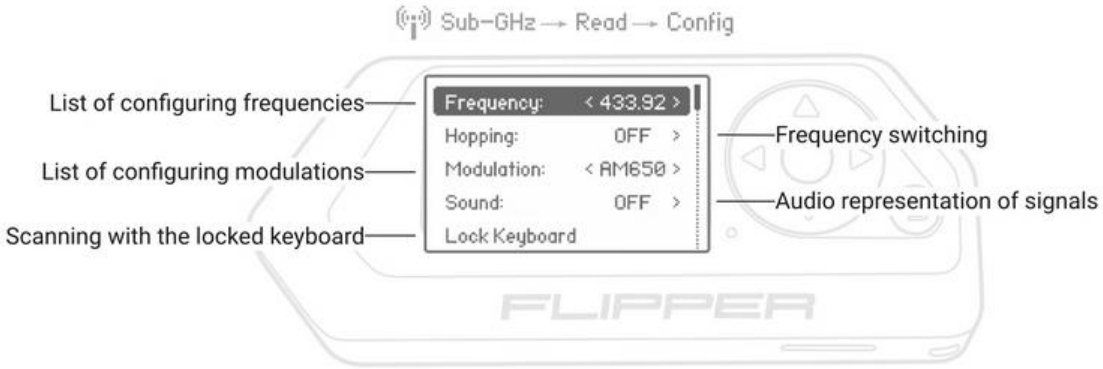
3.3.1 Lire une fréquence

Le Flipper peut lire des protocoles préenregistrer, et il existe donc des protocoles que le flipper ne connait pas. Si tel est le cas passer au sous chapitre suivant.

Pour commencer dirigez-vous dans **Sub-GHz → Read** à ce niveau il commence déjà à lire une certaine fréquence.



Dans **Config** vous pouvez choisir d'autre fréquence.



Lorsque les signaux son capturé, vous pouvez sélectionner le bon signal (s'il en existe plusieurs).

Et enfin l'enregistrer ou l'émuler.

3.3.2 Lire une fréquence Brute

Lire une fréquence Brute permettra de lire et enregistrer n'importe quel signal si jamais le flipper ne dispose pas du protocole que vous essayez de percevoir avec le chapitre précédant.

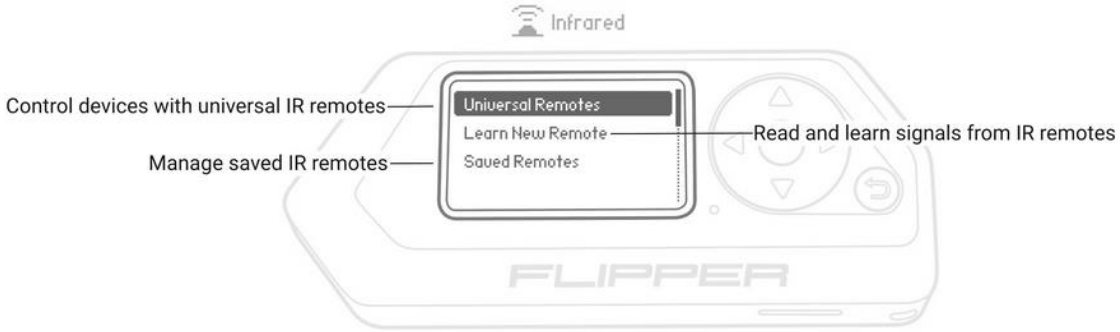
Pour cela dirigez-vous dans **Sub-GHz → Read Raw** et enfin lancer **REC** tout en utilisant votre badge stopper votre signal sur **Stop** et enregistrer **Save** votre signal.

Vous pouvez ensuite utiliser votre signal dans **Sub-GHz → Saved**.

3.4 Infrarouge

L'infrarouge nous l'utilisons au quotidien que ce soit pour utiliser notre télévision, les vidéos projecteurs ou encore votre Box TV.

Cette infrarouge est principalement utilisée dans nos télécommandes ou encore comme exemple dans les jeux vidéo avec le Track IR permettant à une personne de bouger sa tête dans les jeux comme dans la réalité.



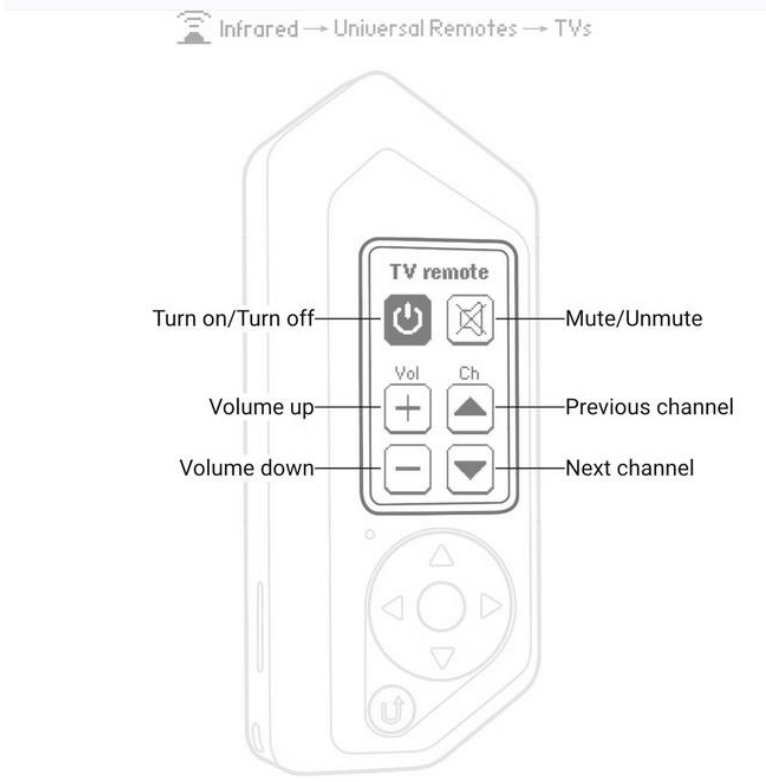
Attention la carte SD est obligatoire pour le stockage des signaux ;

3.4.1 Universal Remotes

Le flipper dispose d'un dictionnaire comportant les protocoles les plus utilisé nous pouvons l'utiliser dans **Infrared → Universal Remotes**

A ce niveau vous pouvez choisir quel type d'équipement vous voulez utiliser.

Après avoir choisi quel équipement vous voulez utiliser, vous disposerez du flipper en mode télécommande.

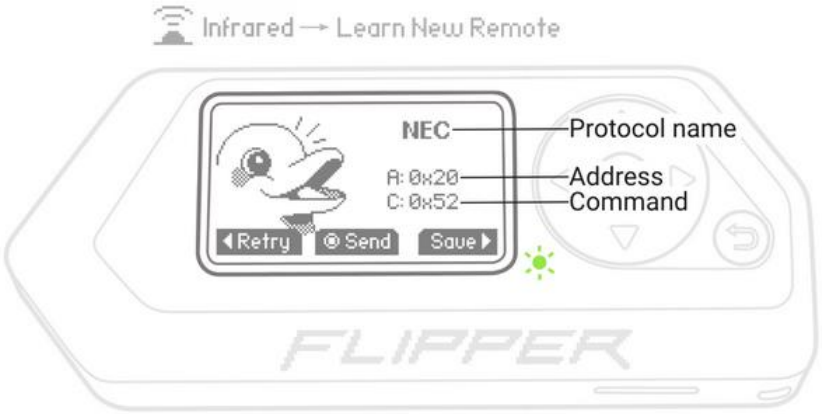


3.4.2 Ajout d'un signal infrarouge

Nous pouvons capturer les signaux infrarouges et les répliquer pour les utiliser à la place de la télécommande maitre.

Diriger vous dans Infrared → Learn New Remote.

Ensuite utiliser un bouton de votre télécommande à répliquer.

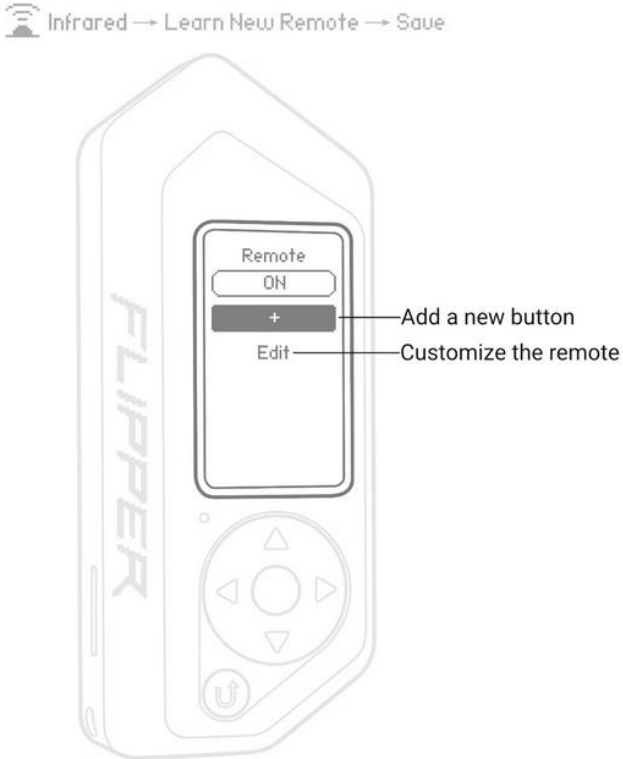


A ce moment votre flipper à capturer le signal pour utiliser le bouton que vous venez d'activer.

Vous pouvez utiliser le signal répliquer → **Send** ou sauvegarder le → **Save**

Vous aurez la possibilité à la suite d'utiliser le signal enregistré ou d'en ajouter un autre.

L'accès aux signaux sauvegardé se fait via **Infrared → Saved Remotes**



 Date : 27/04/23

3.5 Bad USB

Bad USB interagi comme un périphérique USB et est reconnu par les ordinateurs comme périphérique d'interface humaine (HID).

On peut lancer des scripts, modifier des paramètre système, ouvrir des portes dérobées bref faire tout ce qu'un humain peut faire avec un accès physique à l'équipement.

Pour l'utiliser, il vous faut développer votre script avec le langage DuckyScript et de le déposer à l'aide du programme QFlipper disponible sur le site officiel.

Bad USB dispose par défaut de d'une démo pour Windows et MAC OS.

Ci-dessous des liens comportant des scripts a tester pour Bad USB sur Windows, Android et IOS :

https://github-com.translate.goog/UNC0V3R3D/Flipper_Zero-BadUsb?_x_tr_sl=auto&_x_tr_tl=fr&_x_tr_hl=fr

https://github.com/I-Am-Jakoby/Flipper-Zero-BadUSB

Lien de la documentions site officiel : https://docs.flipperzero.one/bad-usb

Attention la carte SD et la mise à jour est obligatoire pour le stockage des scripts.

Attention Bad USB s'exécute comme un clavier qwerty veuillez donc installer le clavier qwerty.

3.5.1 Utilisation de Bad USB

Veuillez à bien brancher votre flipper a l'équipement sur lequel vous voulez exécuter le script.

Pour cette démo nous utiliserons le script demo_windows présent par défaut dans le Flipper.

Dirigez-vous dans **Bad USB → demo_windows** au lancement du script.

Une fois lancer il vous suffit d'attendre que le script soit fini avec le pourcentage afficher sur le Flipper.

3.6 iButton

L'iButton est un type de capteur électronique compact et autonome, qui peut être utilisé pour stocker des données ou pour contrôler des processus industriels. L'iButton est équipé d'une puce électronique qui contient un identifiant unique, ainsi qu'une mémoire pour stocker des données. L'iButton est populaire dans le domaine de la sécurité informatique pour stocker des clés de cryptage et d'authentification. Il peut être facilement intégré dans des applications existantes grâce à sa petite taille et à son interface robuste.

Aucune documentation a été faite pour cause que nous ne disposons d’aucun outils iButton.