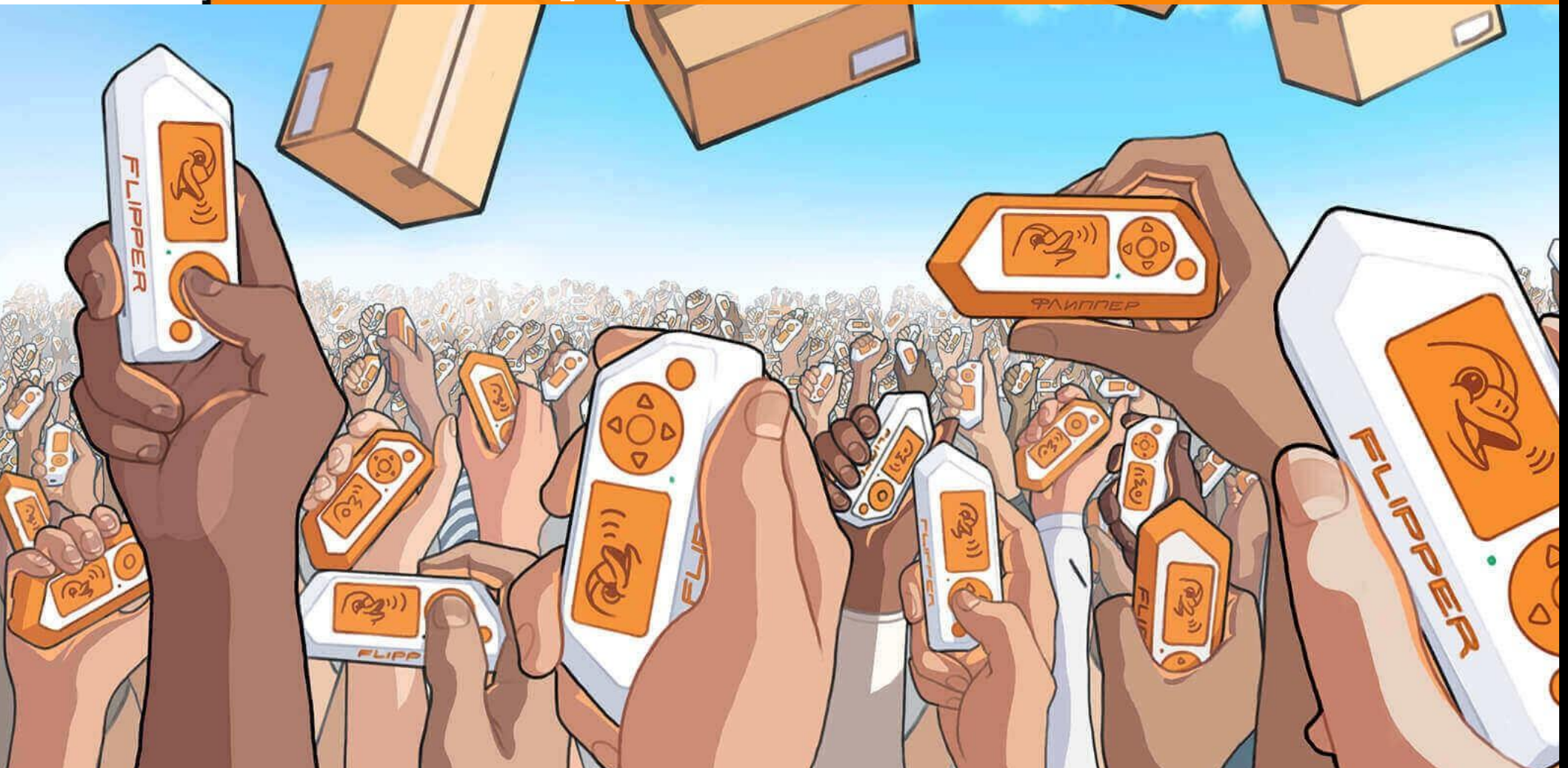
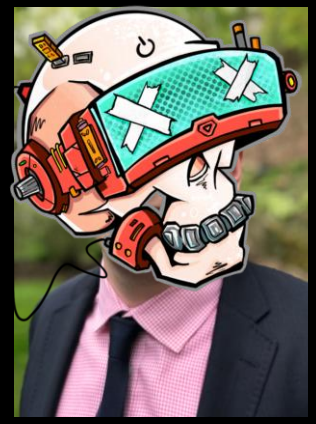
Flipping Locks: Remote Badge Cloning with the Flipper Zero and More



Meet Your Speakers

Langston “sh0ck” C.
OSCP, OSWP, eCPPT, etc.
Senior Red Team Operator



Dan “jcache” G.
OSCP
Principal Penetration Tester


LUMON
hello, my name is
MARK SCOUT SVR'D ACCESS
employee code
08-927
signature


ESP-RFID-Tool
RFID-TOOL
www.RFID-Tool.com


Pairing code:
123 456
FLIPPER


USB Rechargeable Battery
MADE IN CHINA

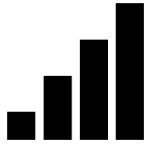
What is RFID Cloning?

- Radio Frequency Identification (RFID) technology supports many physical access control systems
- RFID access control technology provides convenient and cost-effective benefits
- These benefits come with many weaknesses
- Numerous implementations of RFID are susceptible to RFID cloning
- Threat actors can surreptitiously clone or copy RFID credentials under certain circumstances

Low Frequency VS High Frequency RFID

125 kHz

Less Secure



Long range

13.56 MHz

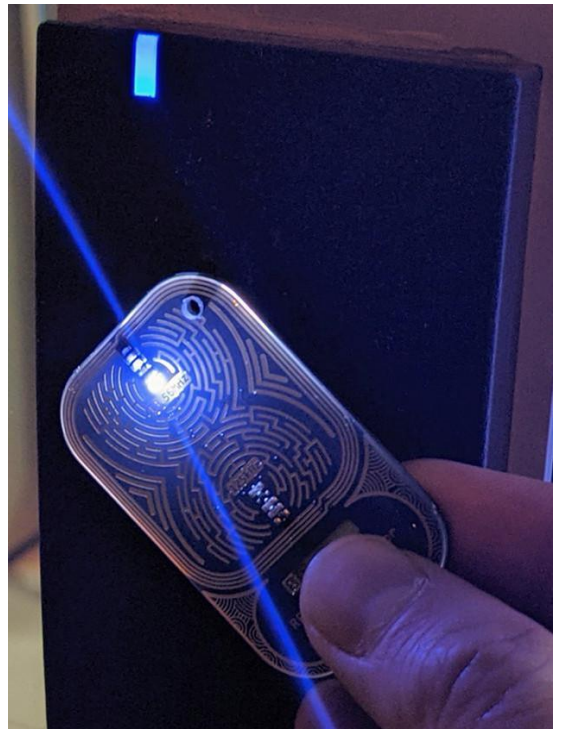
Secure

Short range

Reader Recon

- Proxgrind RF Field Detector

Red LED = 125Khz (Unencrypted)



White LED = 13.56Mhz (Encrypted)

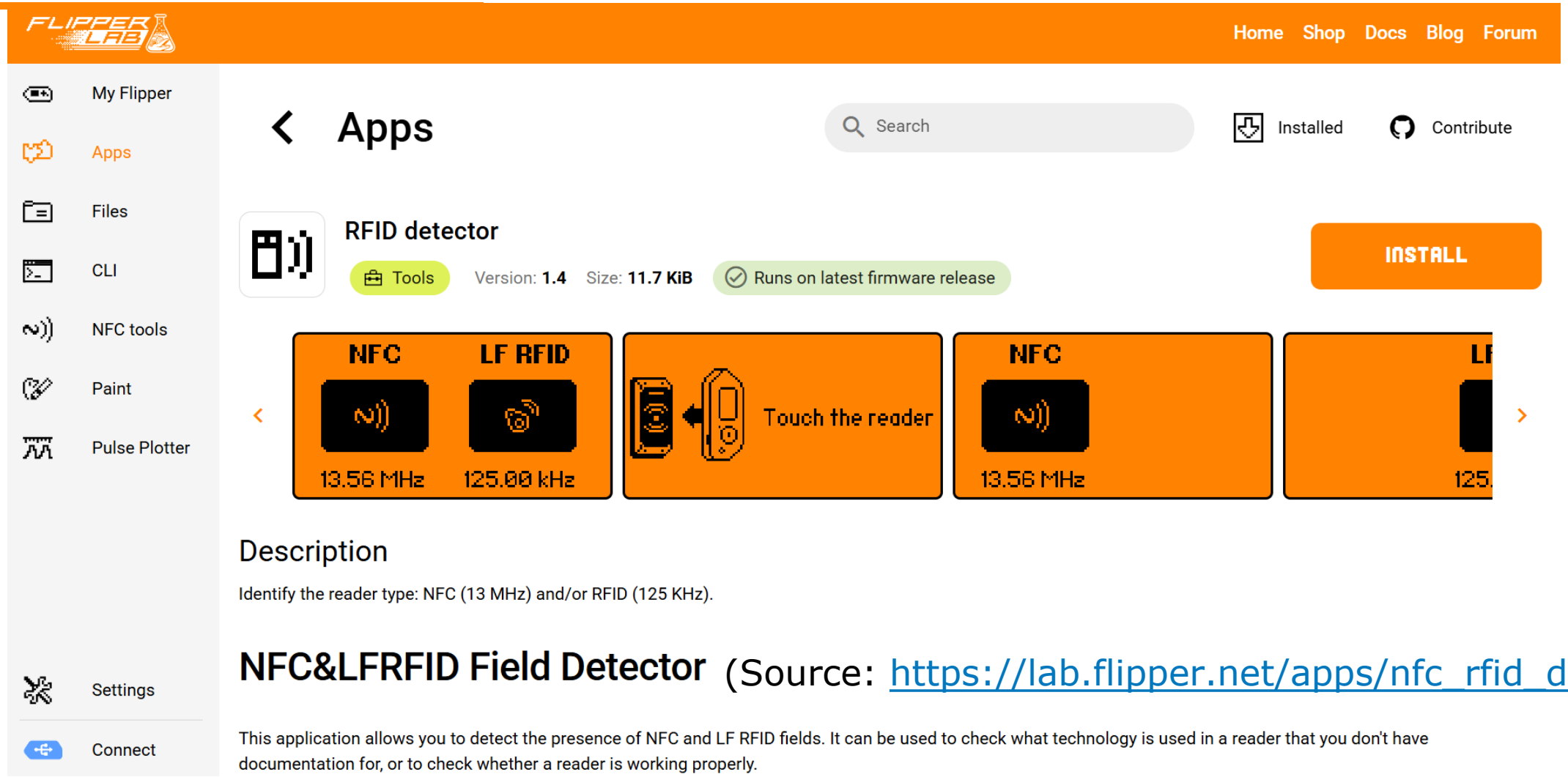
Tutorial: https://www.youtube.com/watch?v=s7gusmY7kwY | Image Src: redteamtools.com

What if it does both?

- Proxgrind RF Field Detector

If it’s red, you’re dead. RIP Physical Security.

Flipper Zero - RFID Detector App



NFC&LFRFID Field Detector (Source: https://lab.flipper.net/apps/nfc_rfid_detector)

This application allows you to detect the presence of NFC and LF RFID fields. It can be used to check what technology is used in a reader that you don't have documentation for, or to check whether a reader is working properly.

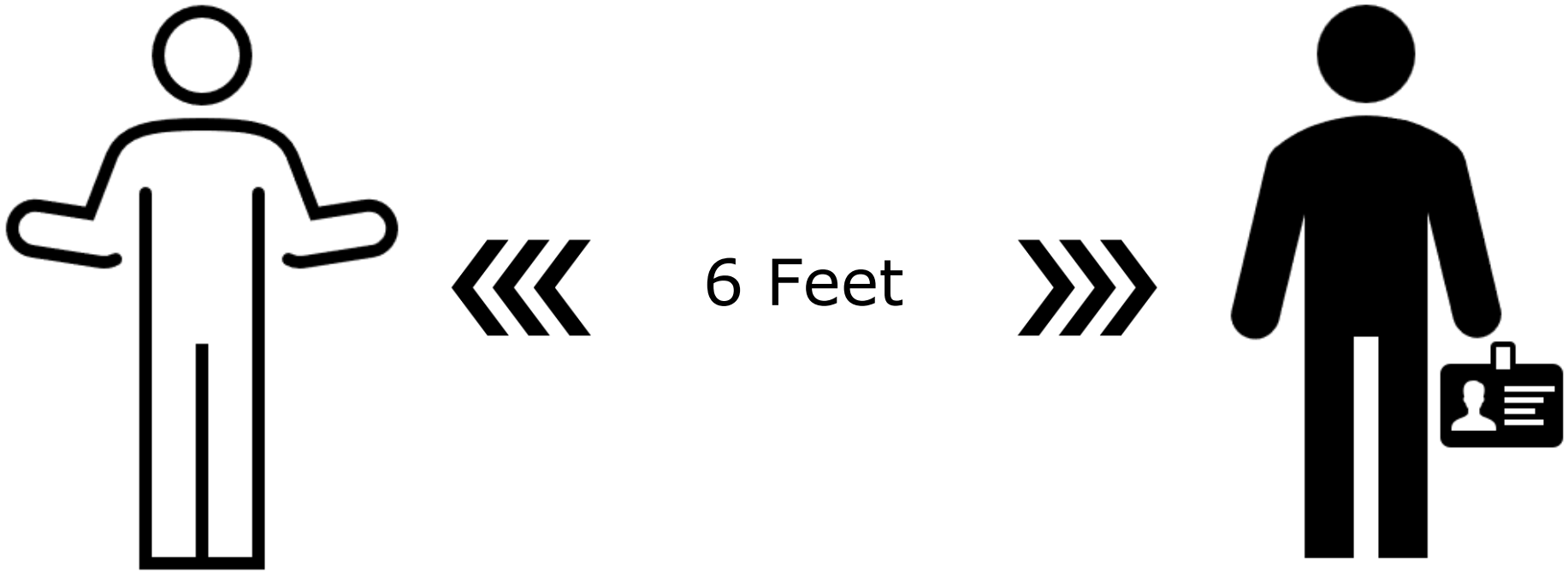
Traditional CQC (Close Quarter Cloning) Methods

Traditional CQC (Close Quarter Cloning) Methods

- **The Brush Pass RFID Method**
  ~ 2’-3’
  - Pros: Very stealthy and fast
  - Cons: Weak Signal Strength and not always socially distanced!
- **Clipboard Cloner Method**
  ~5"-7"
  - Pros: Portable and high signal strength
  - Cons: Less stealthy and not socially distanced!

The Pandemic

The Initial Problem



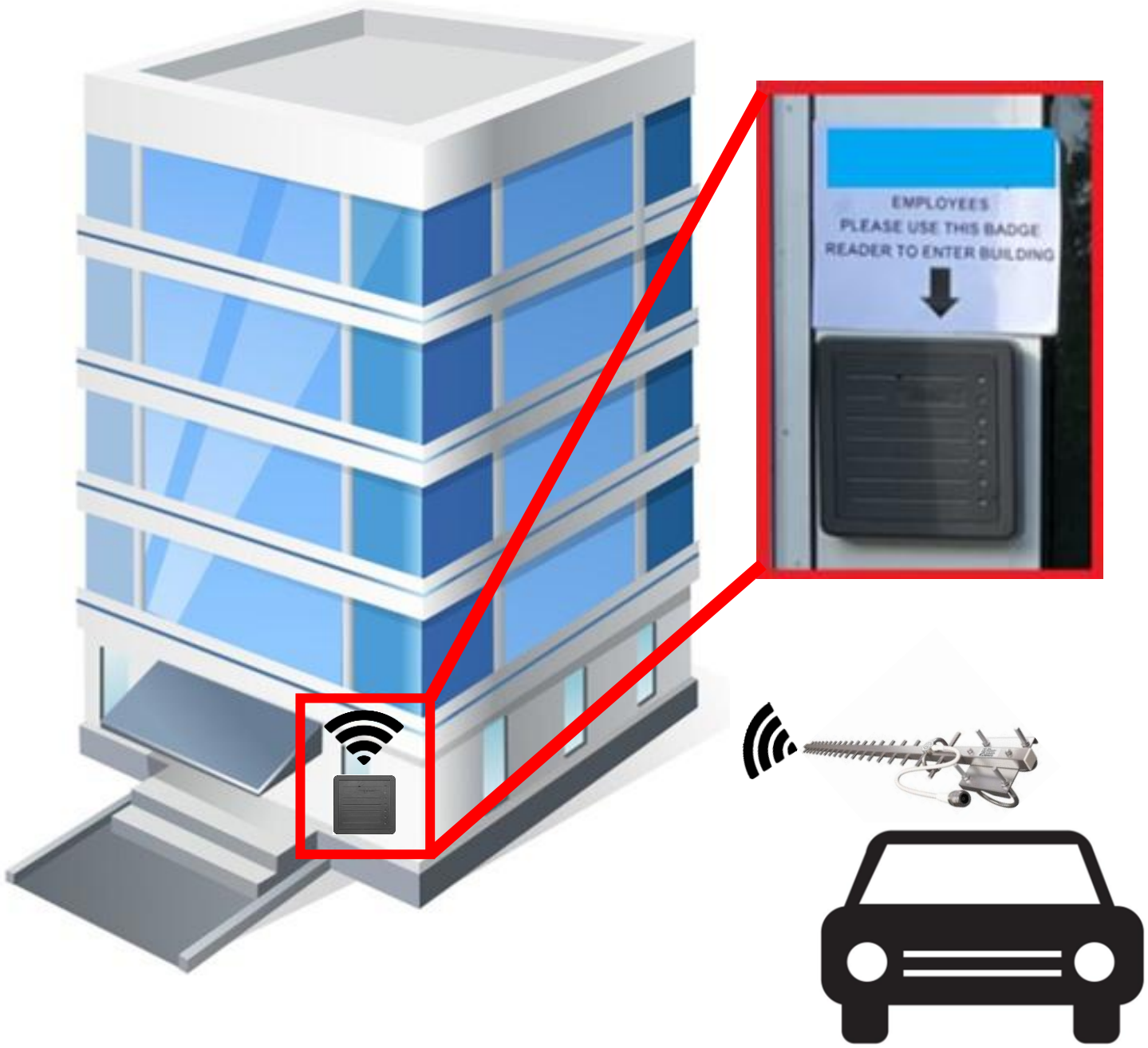
Badge Cloning without Boundaries
(6ft and Beyond!)

The Stand-Alone Wall Reader Implant

- Allows credential collection with little to no human interaction.
- Very stealthy, testers maintain anonymity.
- Remotely collect badge credentials through secure WiFi.

Grab the Loot!

- Remotely Collect Card/FOB Key Loot from the ESP RFID Tool WiFi!
- Grab your favorite long-range antenna and wait!

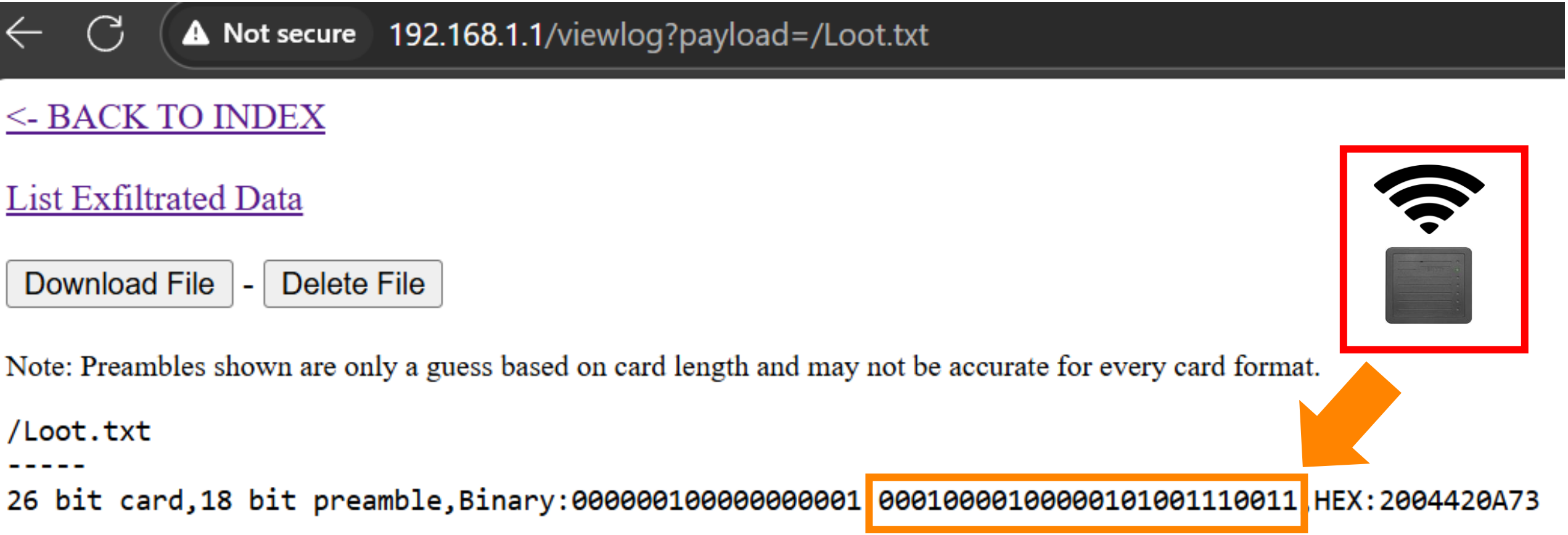


Rogue Reader Wireless Interface

- RFID ESP Key WiFi Access
  - SSID: "ESP-RFID-Tool"
    URL: http://192.168.1.1
- Default credentials to access the configuration page:
  - Username: "admin"
  - Password: "rfidtool"
- Change SSID to blend in with target organization
- Access Card Data in the "List Exfiltrated Data" Page

https://github.com/rfidtool/ESP-RFID-Tool

Rogue Reader Wireless Interface

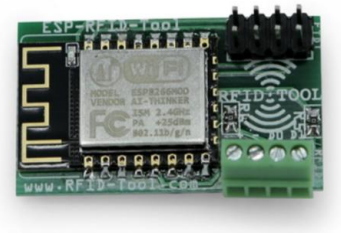


- Copy the Binary Code Payload for later!

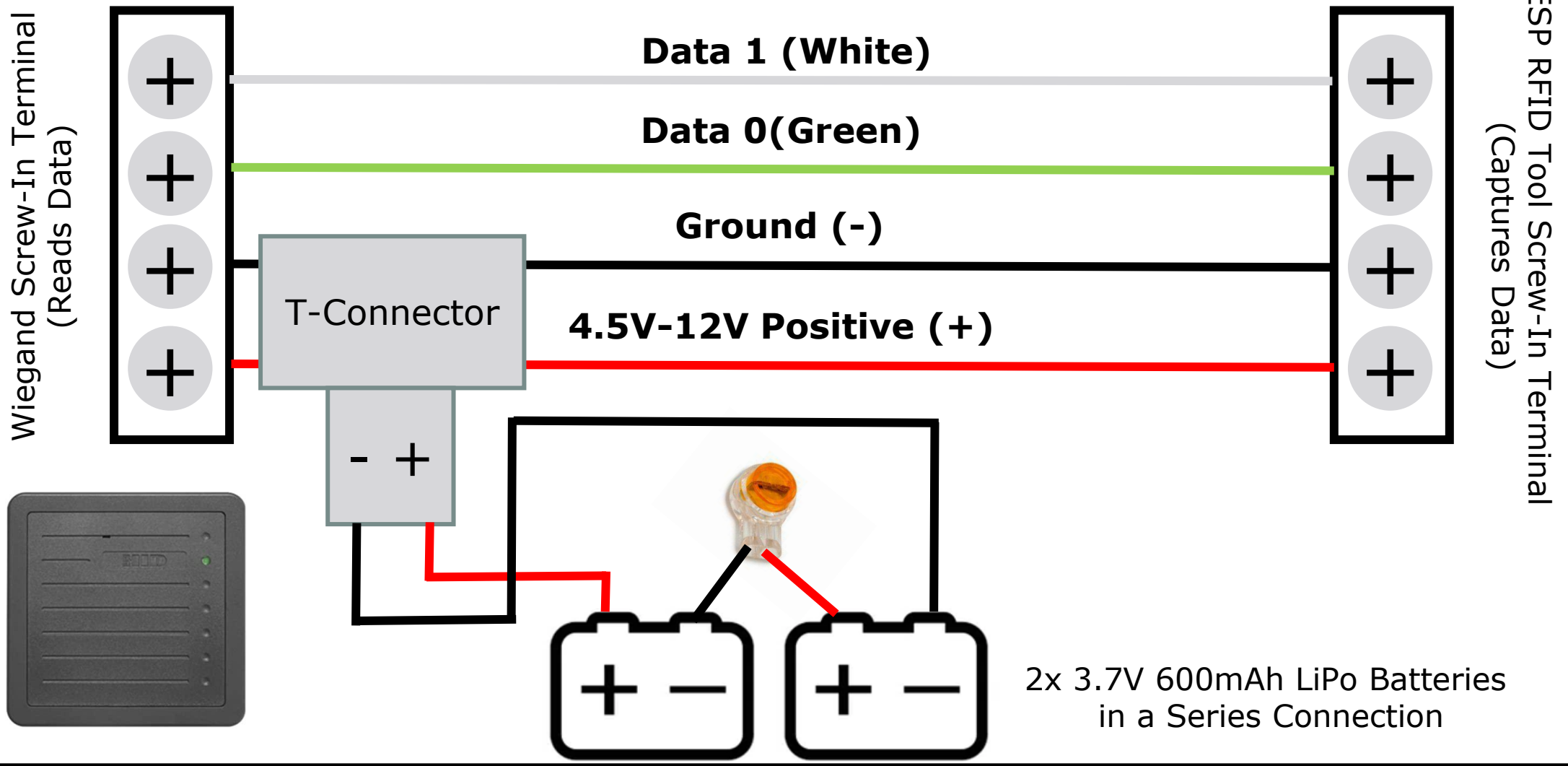
Wall Reader Build – No Soldering Needed!

Low Frequency BOM (Build of Materials):

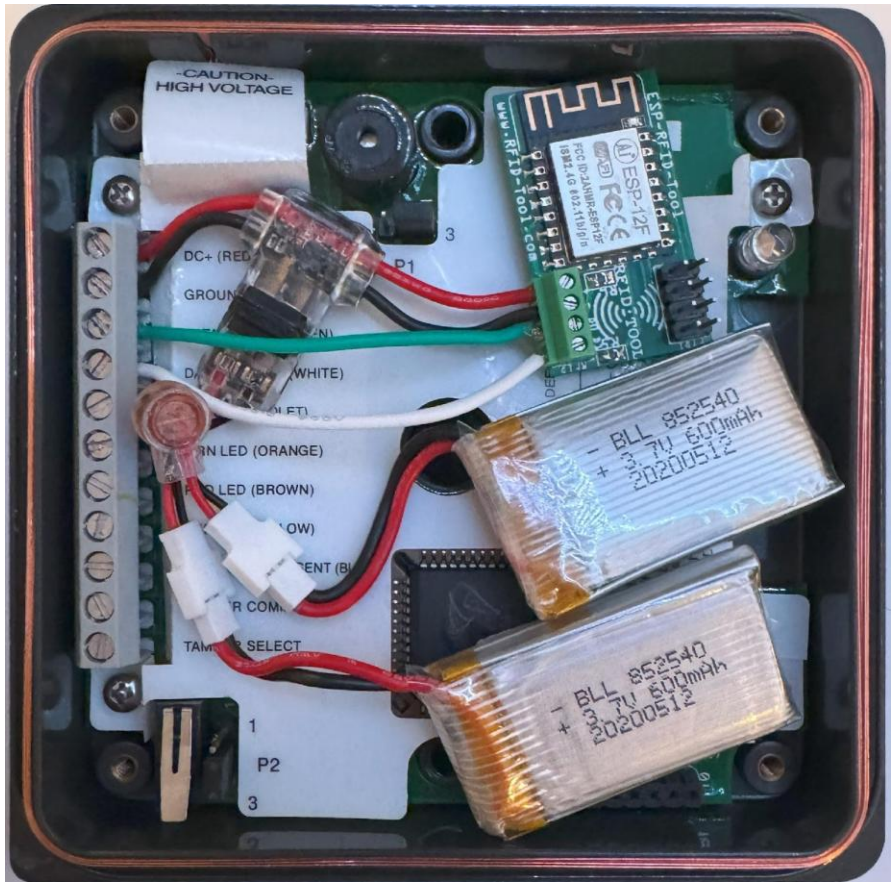
- HID Prox Pro 5355AGN00 Reader
- ESP RFID Tool OR ESPKey
- 3M Wall Hanging Strips
- 2x 3.7V 500mAh LiPo Batteries w/ JST connector
- 1x T Tap Connector
- 2x UY Wire to Wire Connector
- Bread Board Jumper Wires
- 22AWG electrical wire



Wall Reader Connection Guide



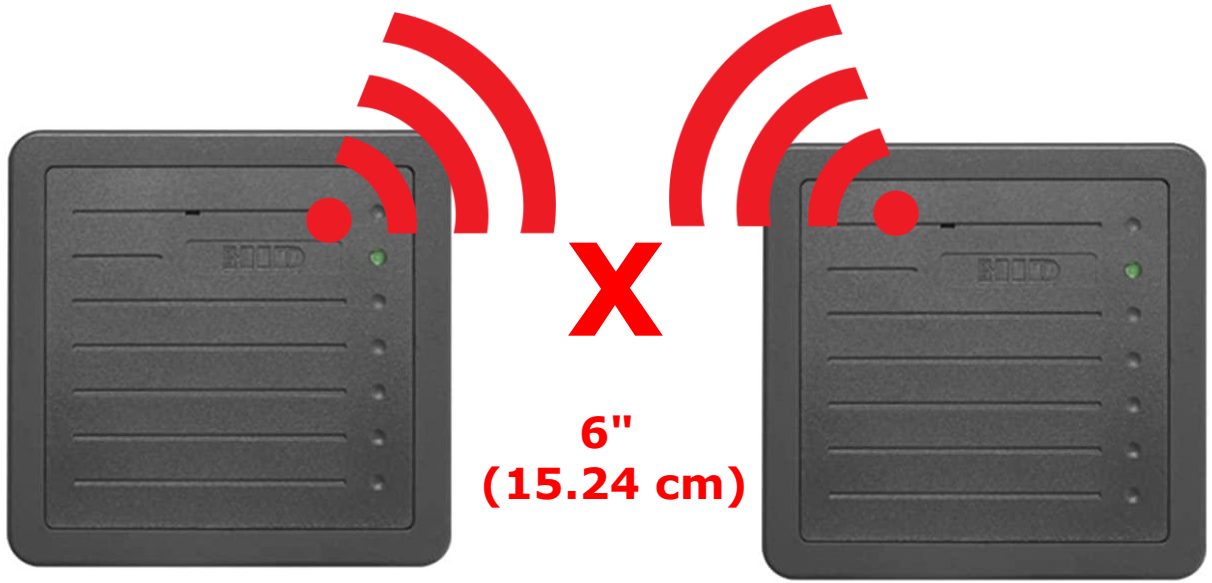
Compact Stand-Alone Wall Reader



Misdirection with Low-Frequency

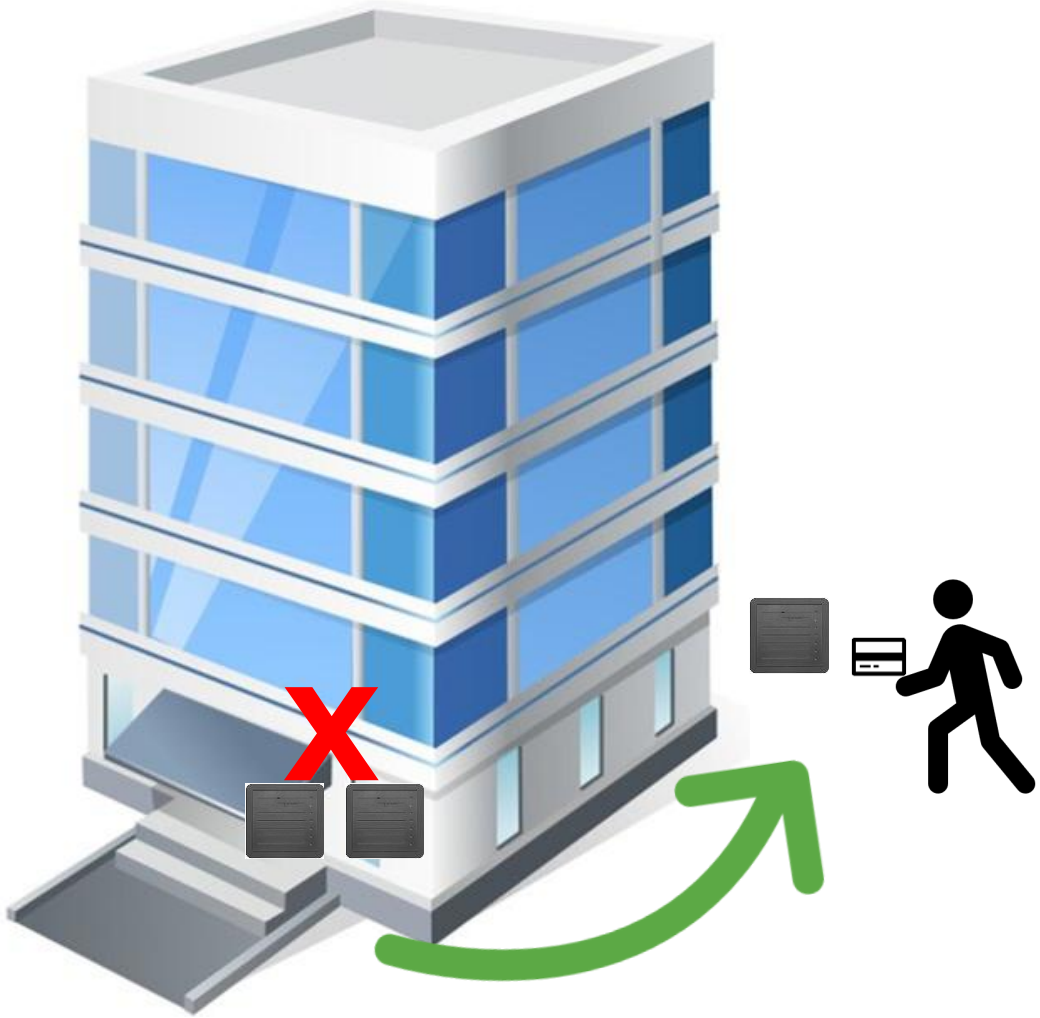
Misdirection – DOSing Readers

- Create a Social Engineering opportunity with a Badge Reader Denial of Service (DoS) attack!
- Placing two Low-Frequency RFID readers within 6" of each other causes interference and will jam the signal from reading card data.



Misdirection – DOSing Readers

- Create a Social Engineering opportunity with a Badge Reader DOS!
- Redirect employees to increase tailgating opportunities!



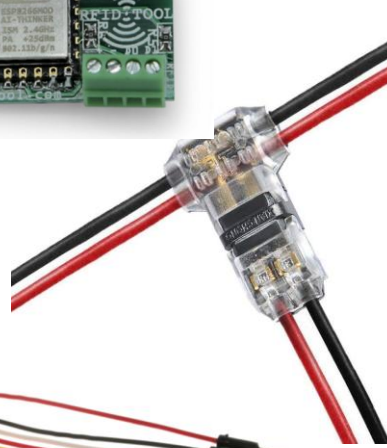
CQC - Clipboard Cloner!

- Take the wall reader build and convert it into a stealthy Clipboard cloning device!

Clipboard Cloner Build

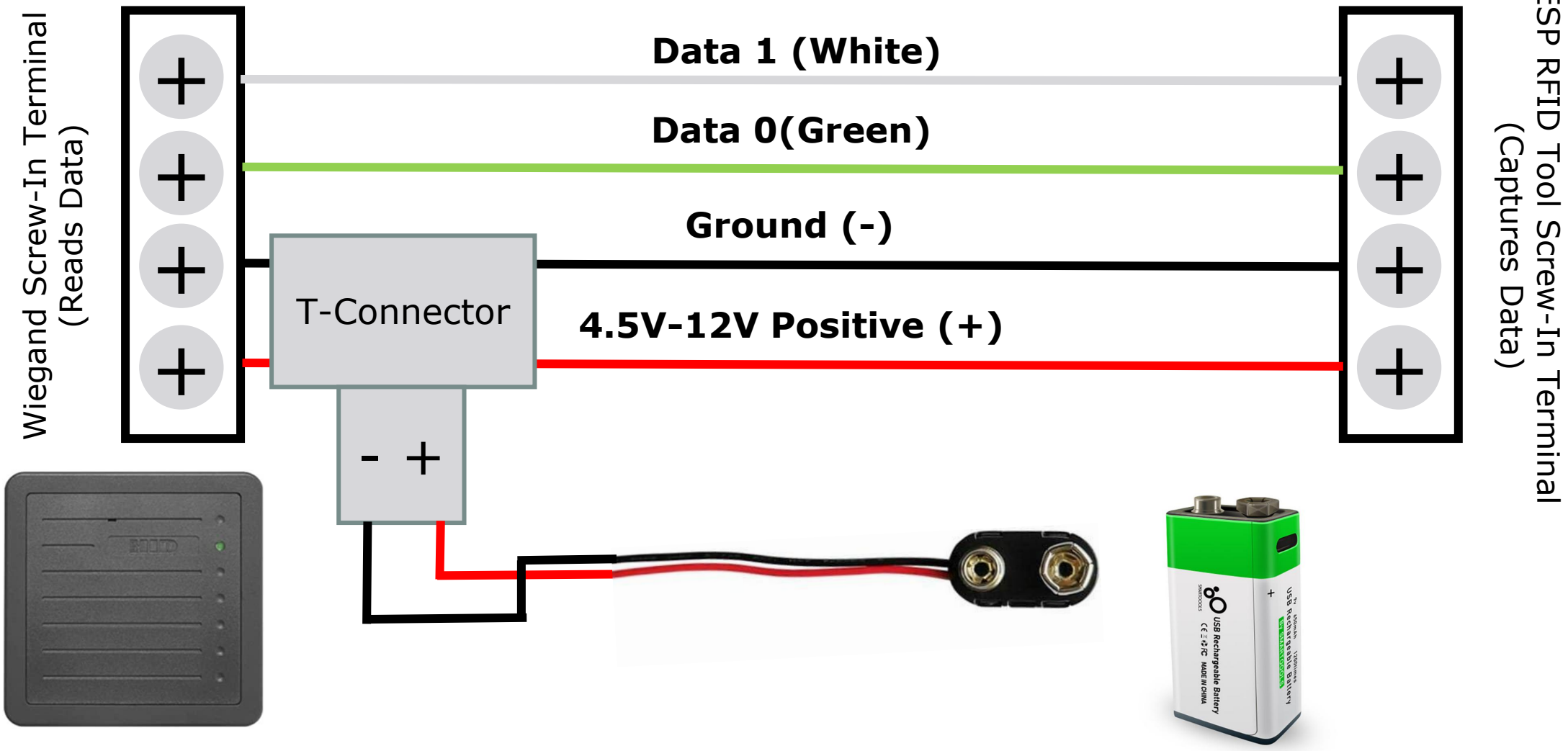
Low Frequency BOM
(Build of Materials):

- HID Prox Pro 5355AGN00 Reader
- ESP RFID Tool OR ESPKey
- 3M Wall Hanging Strips
- 1x 9V 500mAh Rechargeable Battery
- 1x T Tap Connector
- Bread Board Jumper Wires
- 22AWG electrical wire
- Officemate Super Storage Supply Clipboard Case



Full Clipboard Cloning build tutorial guide:
http://www.github.com/sh0ckSec/ClipboardCloner

Clipboard Connection Guide – 9V Battery

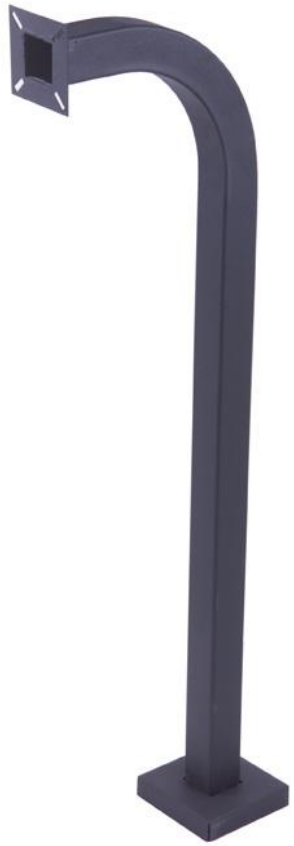


Introducing the Gooseneck Reader

The Gooseneck Reader

Simple, yet effective!

- Gooseneck Pedestal
- Long Range Reader
- Plywood
- Rubber Feet
- Spray Paint



The Gooseneck Reader

- Mobile Long-Range Reader for both Low or High Frequency
- Reads up to ~3.3' (1M) Away
- 12 Hour Battery

The Gooseneck Reader

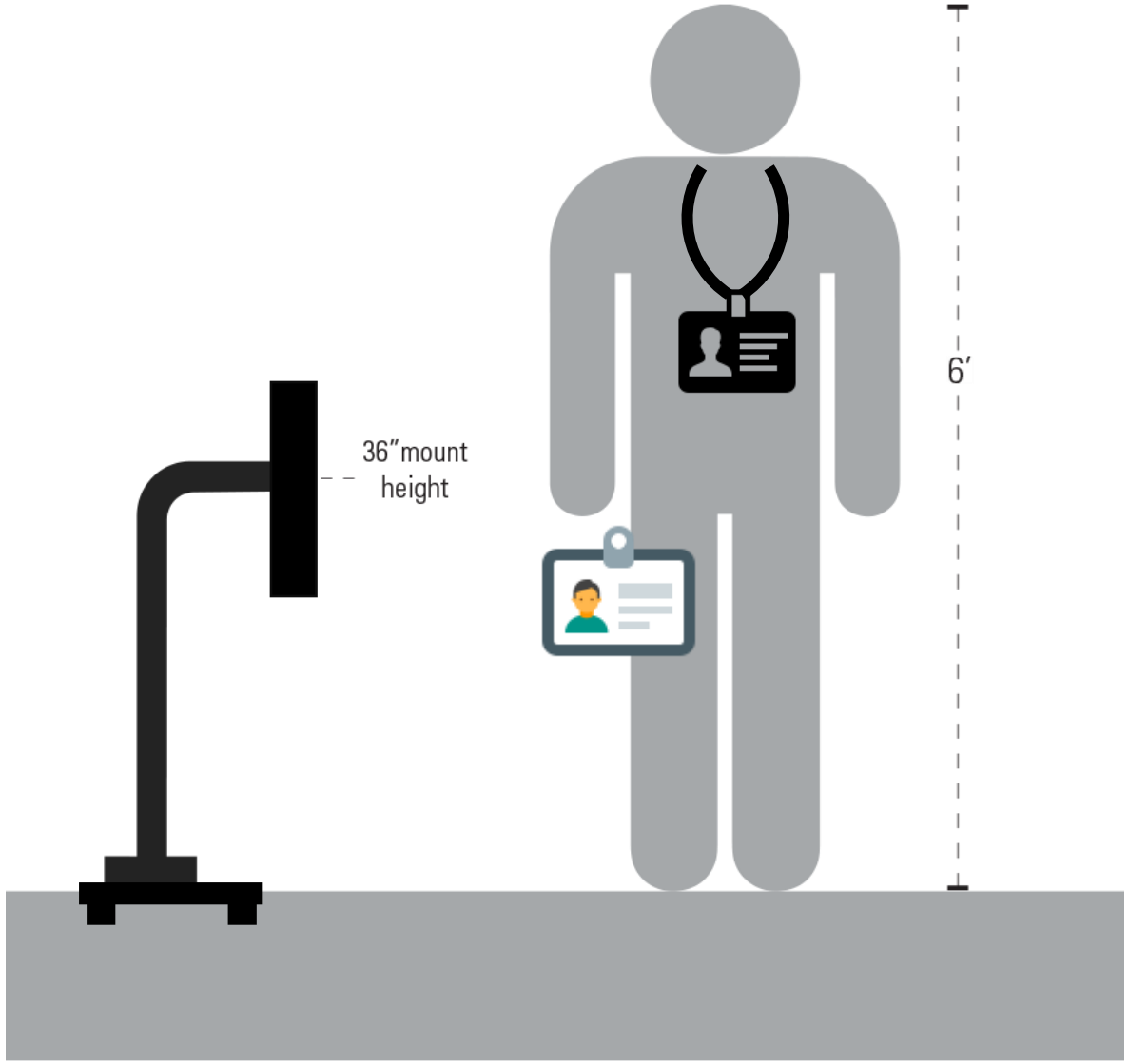
- Mobile Long-Range Reader for both Low or High Frequency
- Reads up to ~3.3' (1M) Away
- 12 Hour Battery

The Gooseneck Reader

- Mobile Long-Range Reader for both Low or High Frequency
- Reads up to ~3.3' (1M) Away
- 12 Hour Battery

The Gooseneck Reader

- Mobile Long-Range Reader for both Low or High Frequency
- Reads up to ~3.3' (1M) Away
- 12 Hour Battery



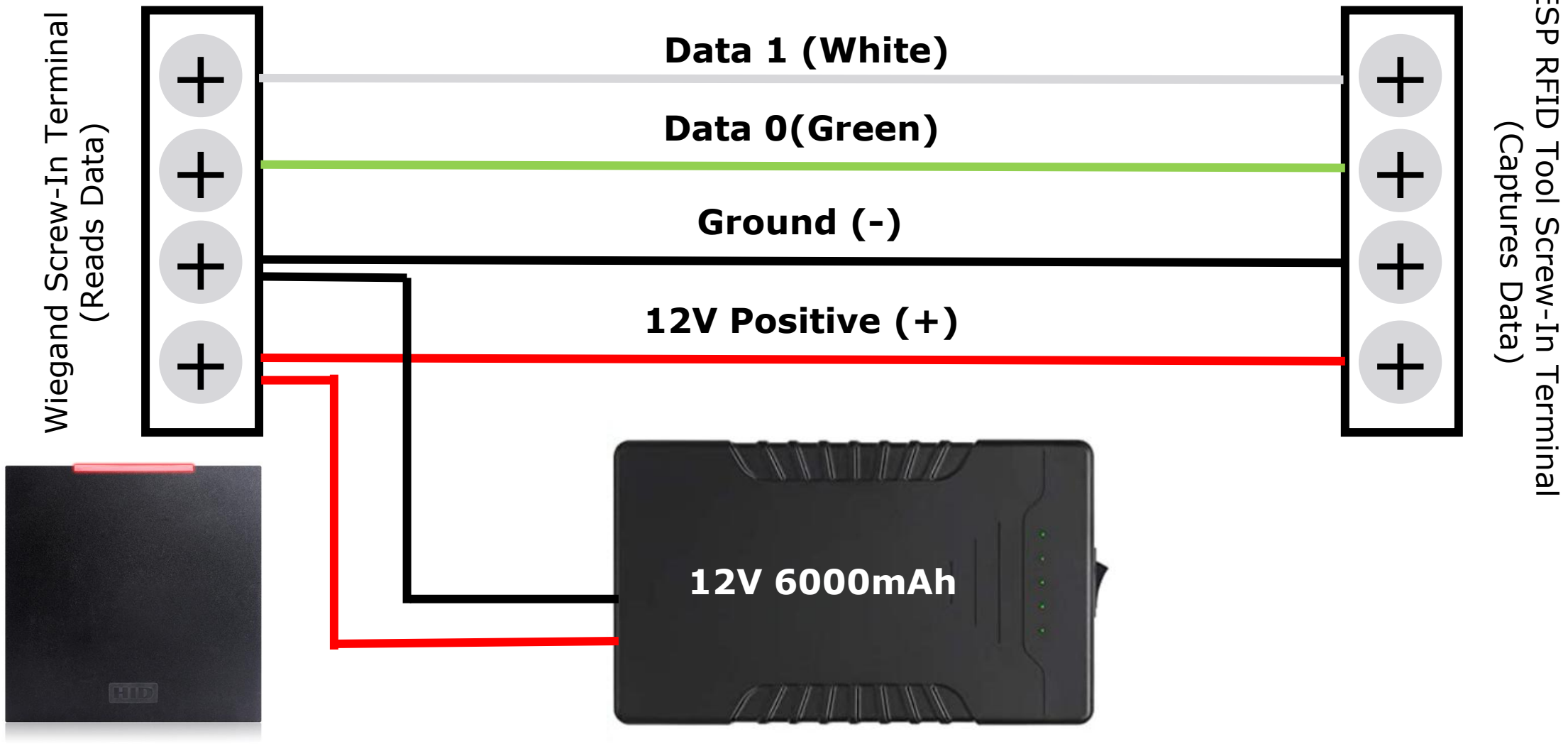
Gooseneck Build – No Soldering Needed!

Gooseneck BOM (Build of Materials):

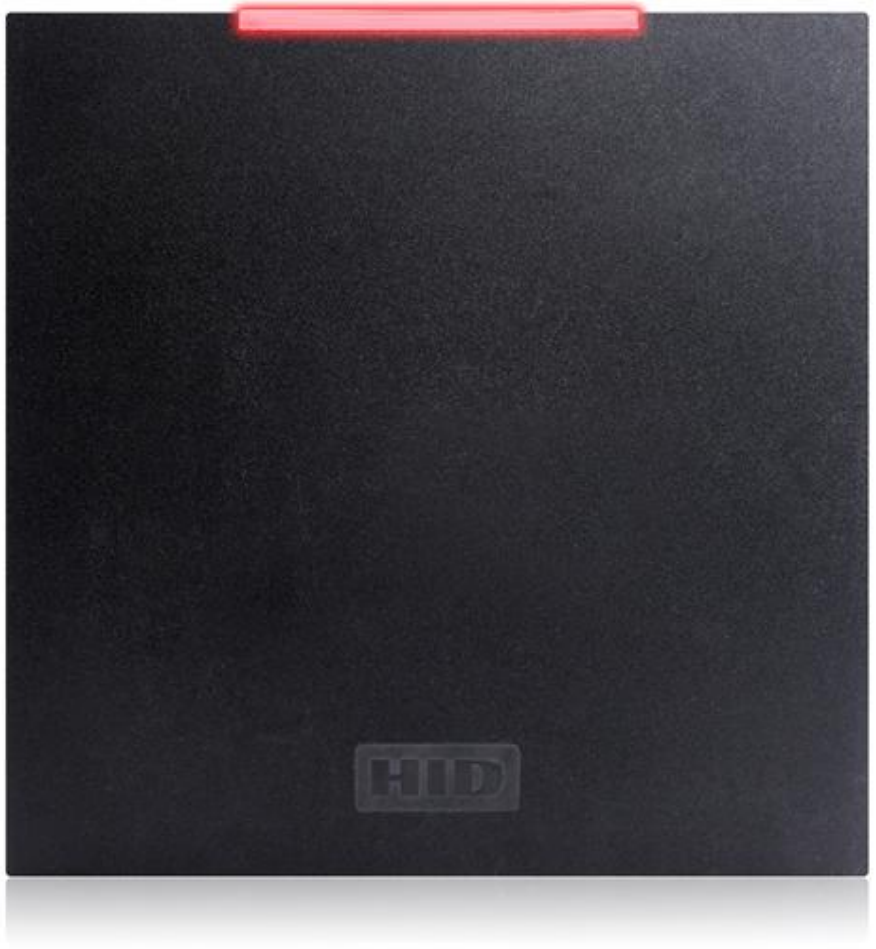
- Low Frequency Long Range Reader
- (e.g. HID MaxiProx 5375)
- High Frequency Long Range Reader
- (e.g. HID iCLASS SE R90)
- MDF or Plywood Wood
- ESP RFID Tool
- 12V 6000mAh/5V 12000mAh DC Battery
- 3/8”x1.25” Nuts and Bolts
- Black Spray Paint
- Bread Board Jumper Wires
- 22AWG electrical wire
- DC Power Pigtail
- Rubber Feet
- Pedestal Pro Gooseneck

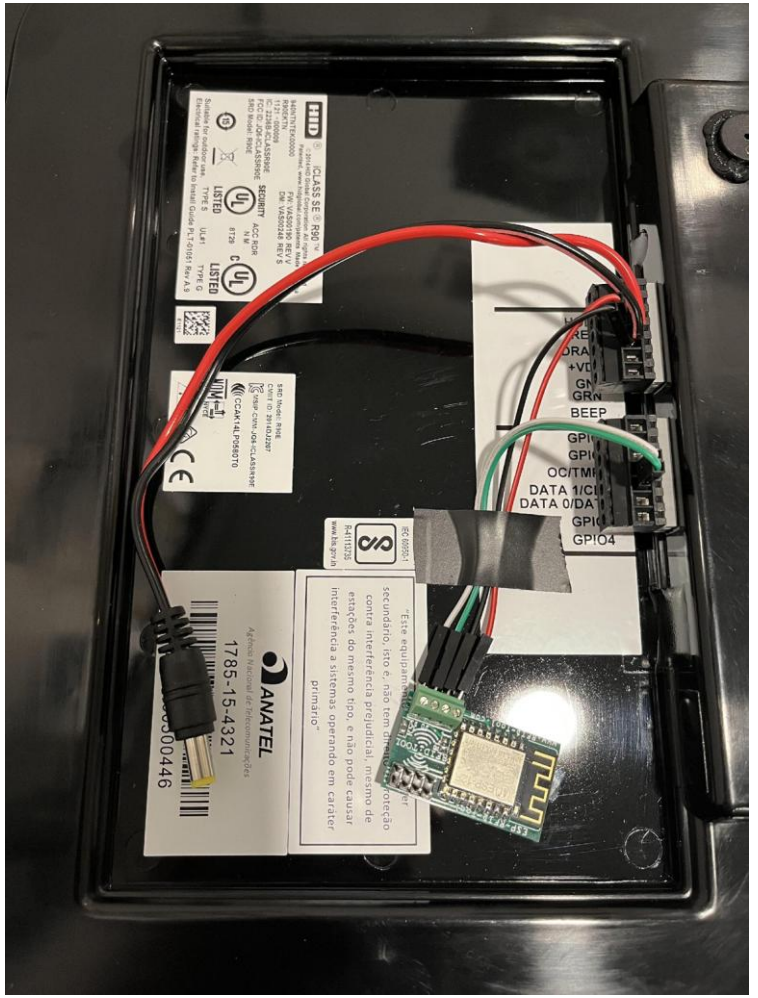
Full build tutorial guide:
www.github.com/sh0ckSec

Long Range Reader Connection Guide

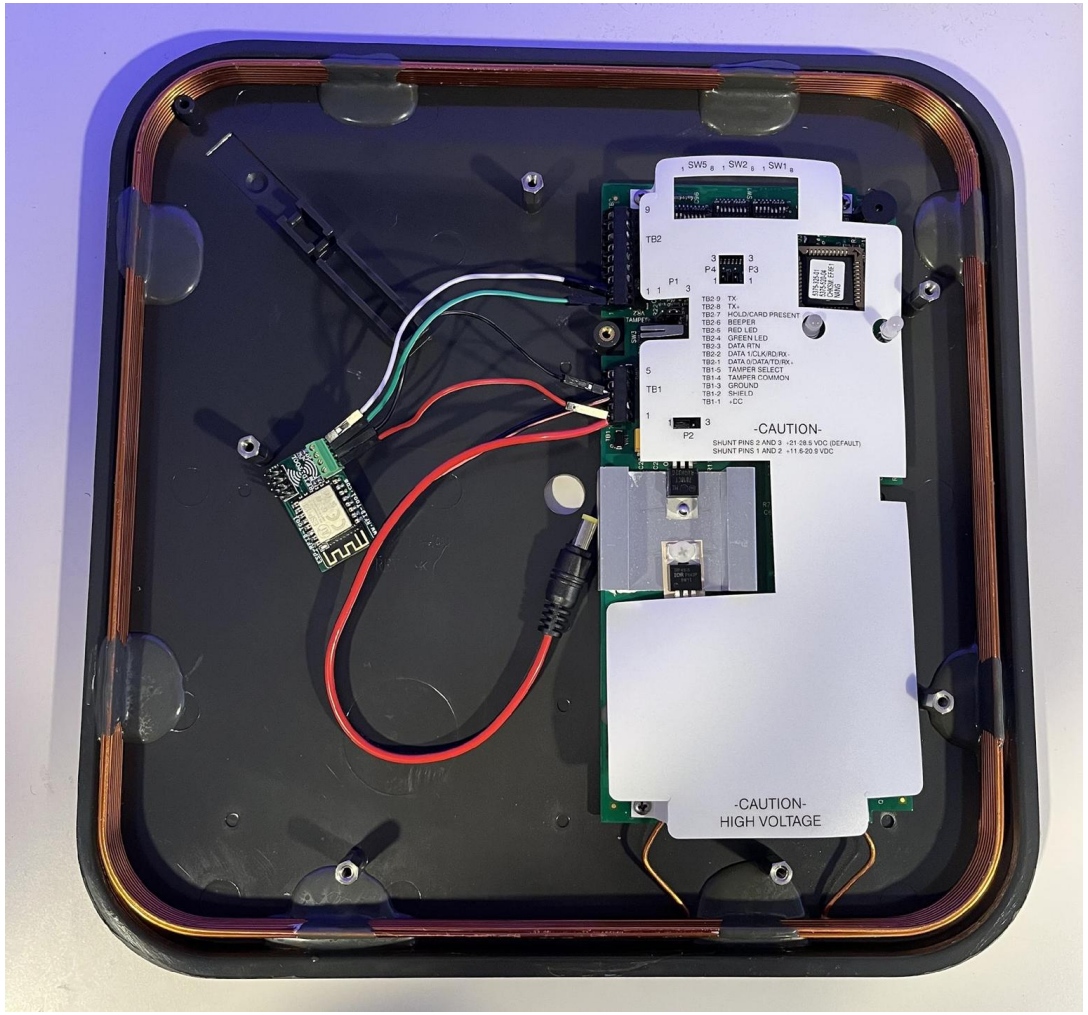


Long Range Reader Wiring





Long Range Reader Wiring

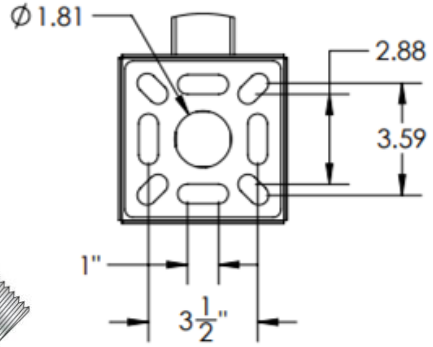


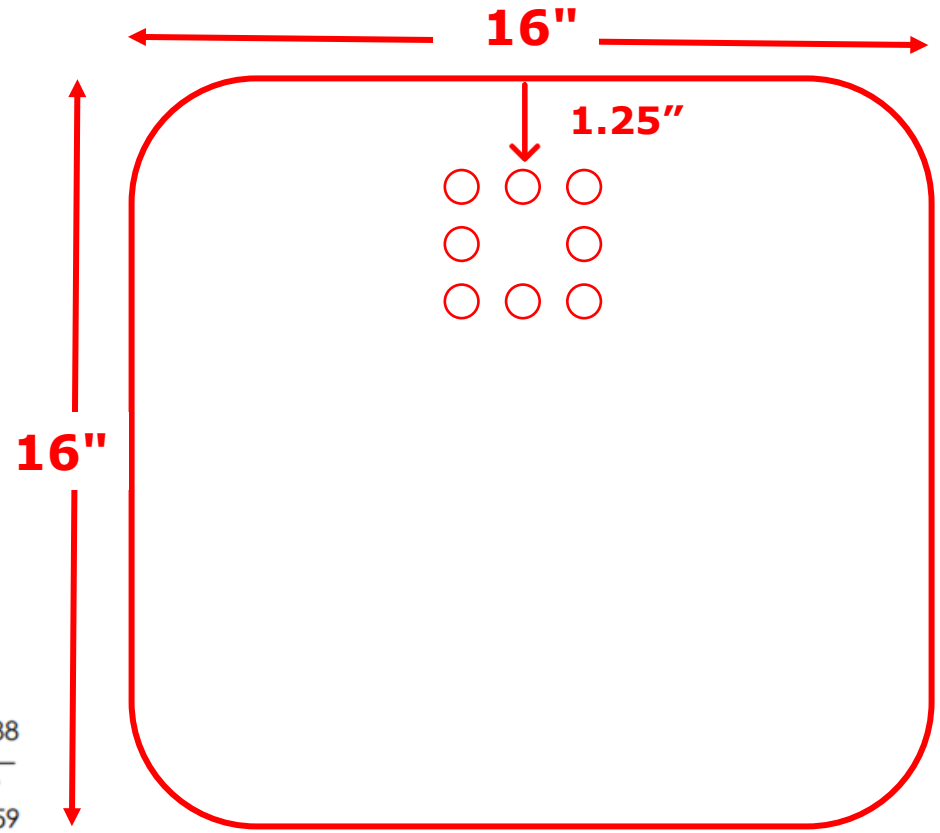
Gooseneck Base

Download the Gooseneck Base MK2 template here for laser cutting, CNC or print, along a full build tutorial guide:
www.github.com/sh0ckSec

Materials:

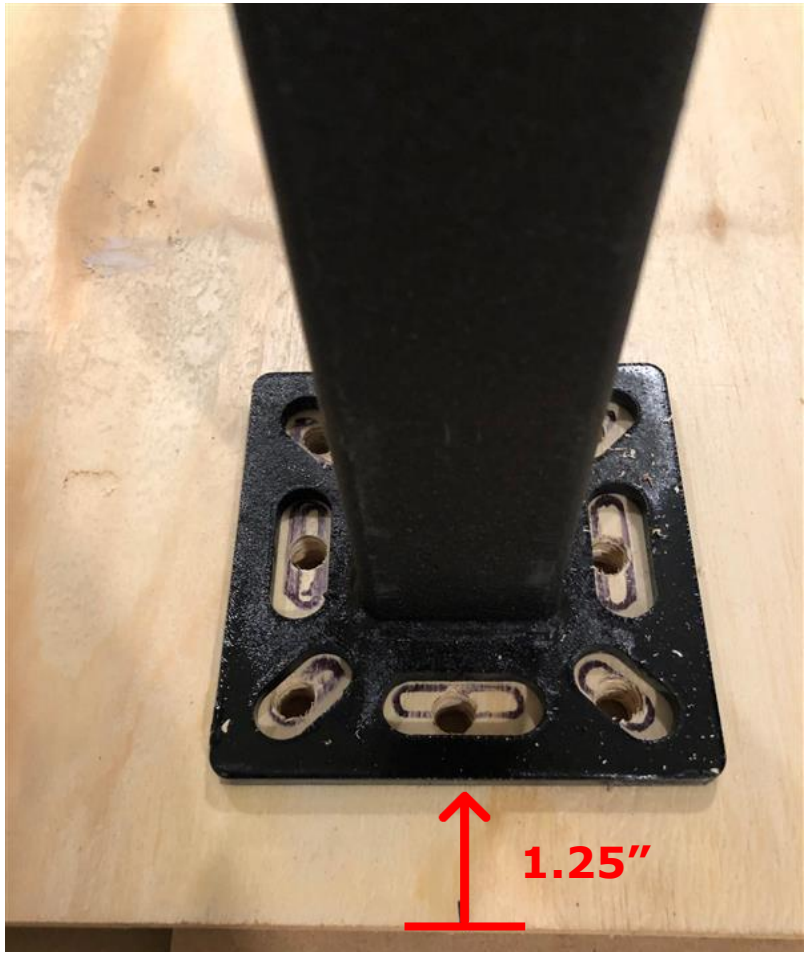
- 30mm Heavy Duty Rubber Furniture Pads
- 3/8” x 1 1/4" Carriage Bolts and Wing Nuts
- ½" thick MDF or Plywood



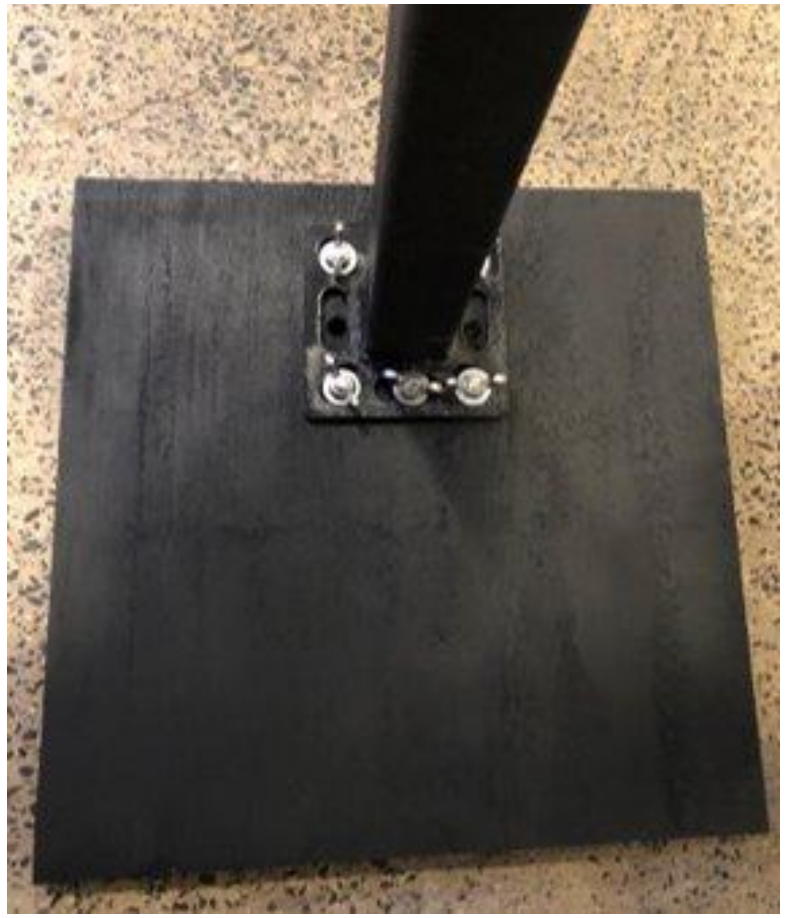


(40.62cm x 40.62cm)

Gooseneck Base – Installation

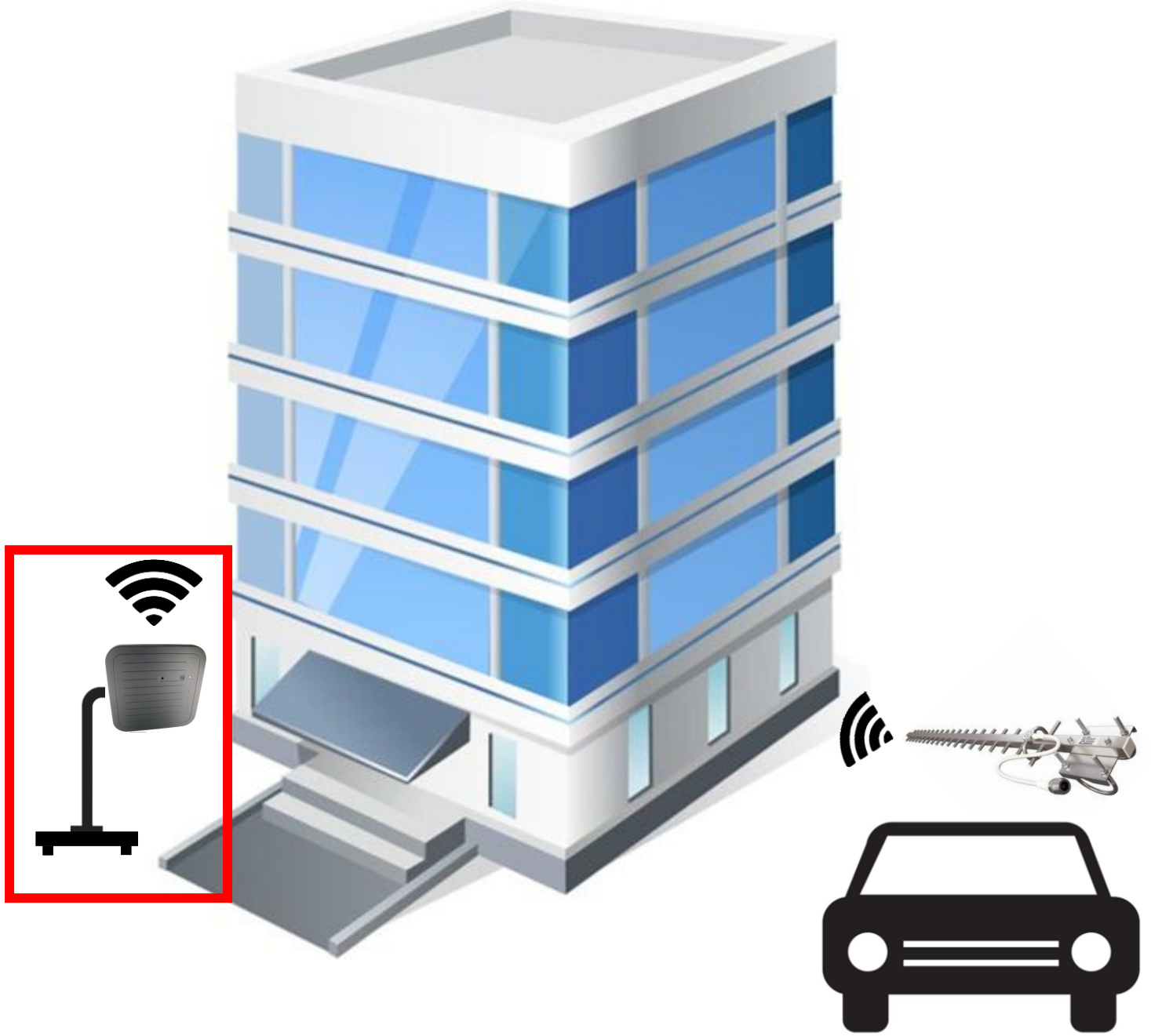


Gooseneck Base – Installation



Grab the Loot!

- Remotely Collect Card/FOB Key Loot from the ESP RFID Tool WiFi!
- Grab your favorite long-range antenna and wait!



Cloning Badge Data with a Flipper Zero

Quick and Easy!

Flipper Zero RFID Copy Method

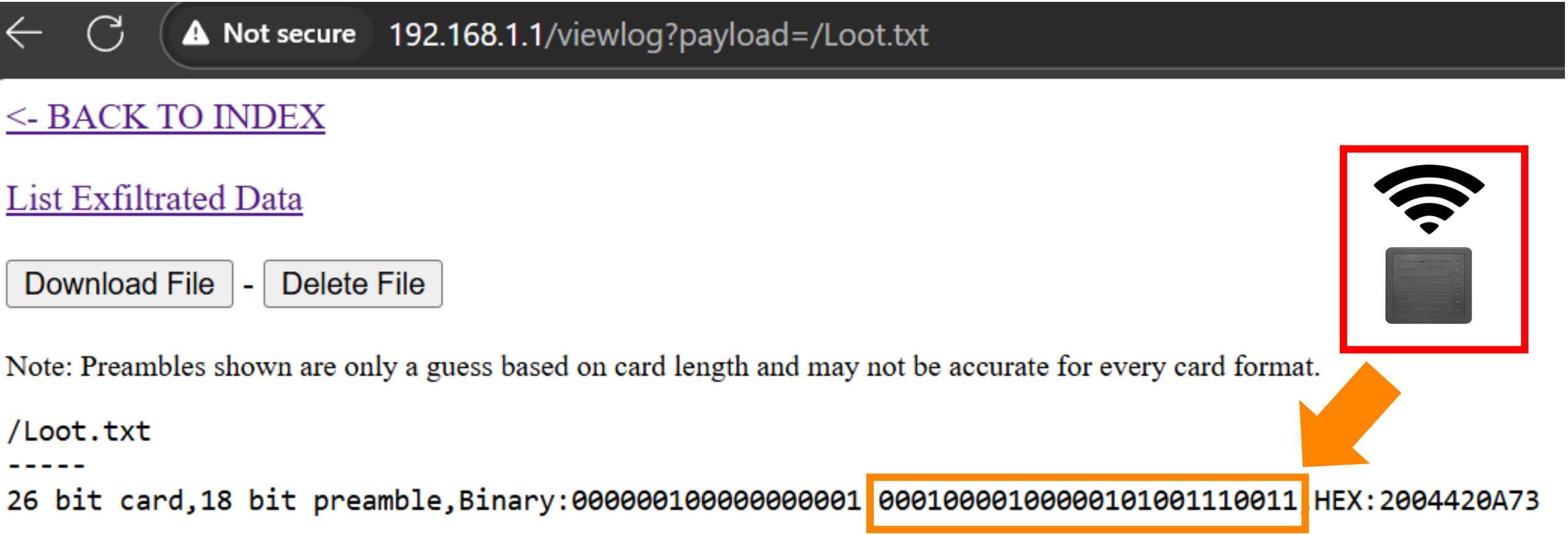
Materials Needed:

- Android Phone/Tablet or iPhone
- Flipper Zero
- Blank T5577 Rewriteable RFID Cards
- Bin-HEX Converter App
- **Flipper Mobile App**
  https://flipperzero.one/

GET IT ON Google Play

Download on the App Store

Rogue Reader Wireless Interface



- Copy the Binary Code Payload for later!

Card Data

1. Facility Code (FC) #0-255
2. Card Number (CN) #0-65,535

Card Number (CN)
(printed on the back of the card)

Facility Code…?

Binary Code Breakdown


```
/Loot.txt
-----
26 bit card,18 bit preamble,Binary:00000010000000001 00010000100000101001110011 ,HEX:2004420A73
```

Standard 26-bit (H10301)

0 00100001 0000010100111001 1

Composed of 1 even parity bit, 1 odd parity bit, an 8-bit facility code, and a 16-bit card number.

Source: https://accessgrid.com/guides/access-control-protocols/examples-of-every-access-control-bit-format

Binary Conversion to HEX for Flipper Zero

```
/Loot.txt
-----
26 bit card,18 bit preamble,Binary:0000001000000000001 000100001000001010011110011 HEX:2004420A73
```

1. Copy the second portion of the binary data:

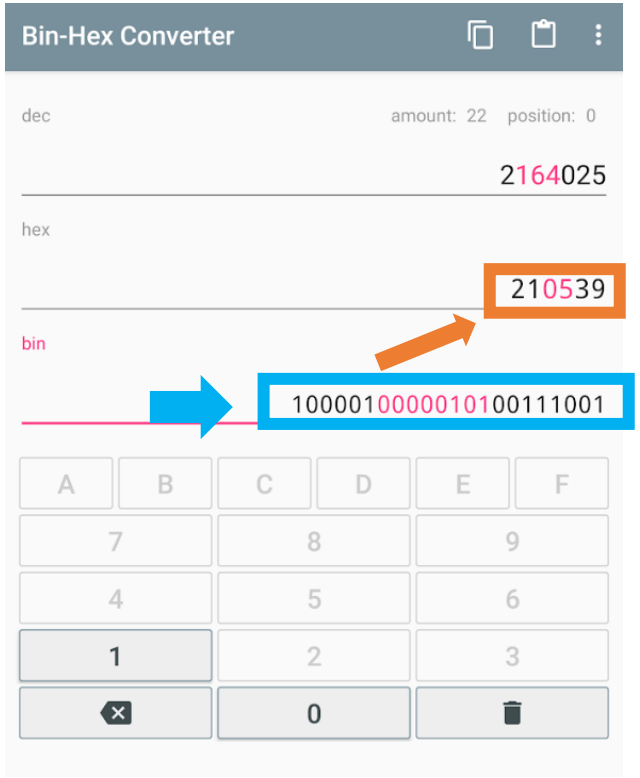
   000100001000001010011110011

2. REMOVE the leading and trailing parity bits:

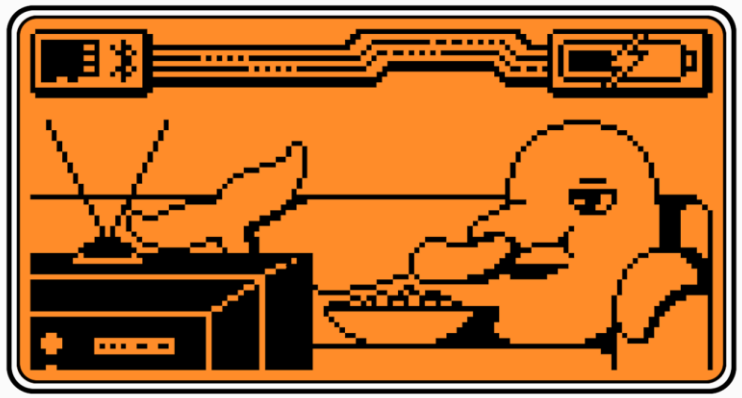
   ~~0~~ **00100001000001010011100 1** ~~1~~

3. Copy this and convert into HEX using a Bin-HEX Converter

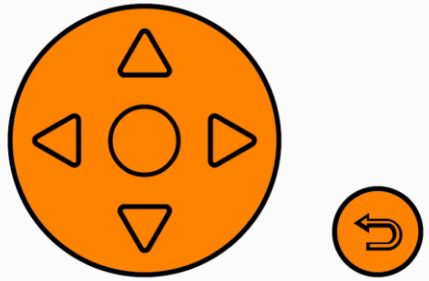
   00100001000001010011100 1 = 21 05 39



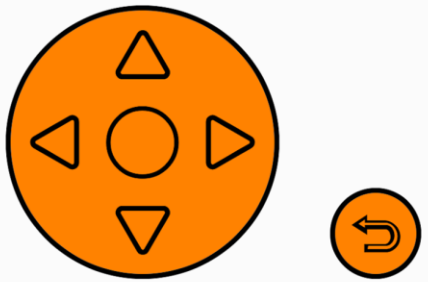
Flipper Zero – Adding Card



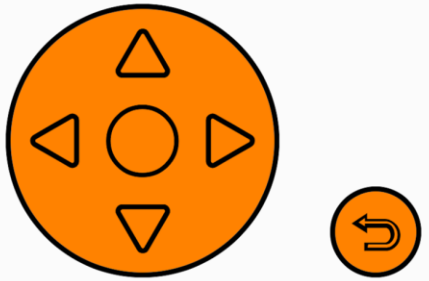
FLIPPER



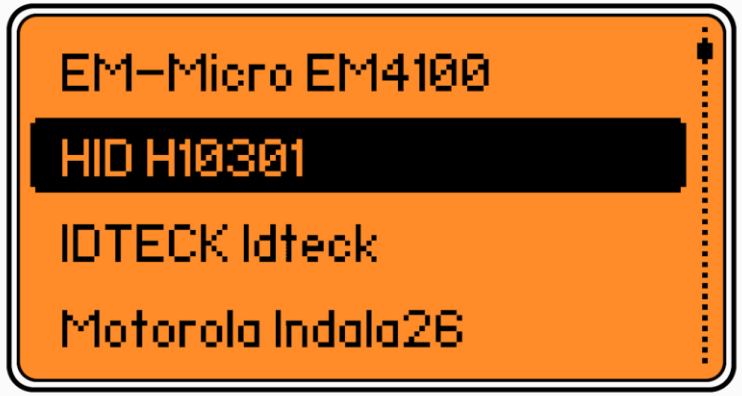
FLIPPER

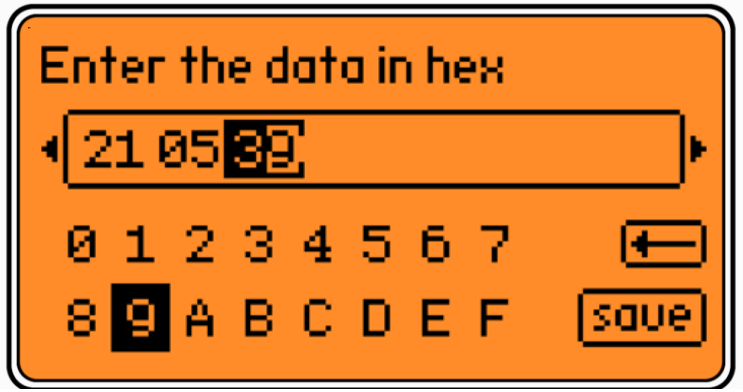


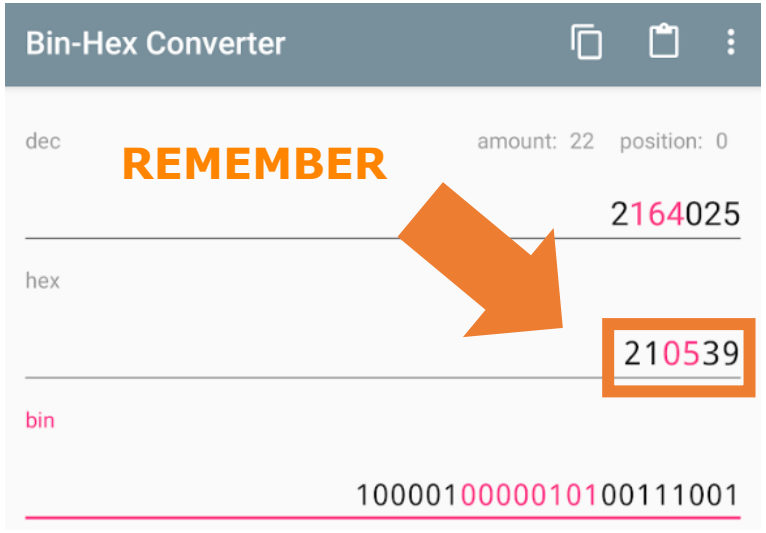
FLIPPER



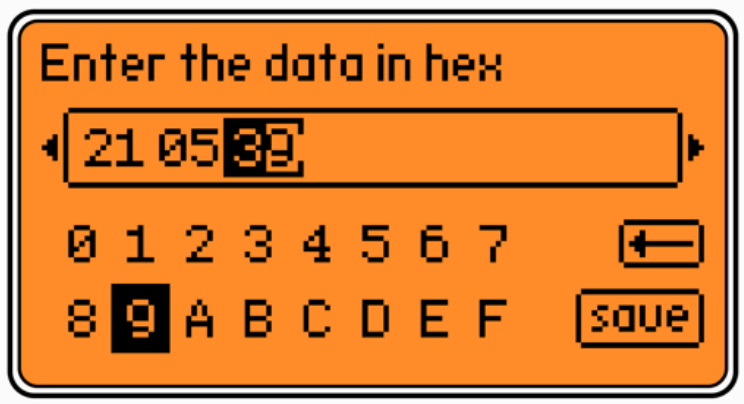
Flipper Zero – Adding Card

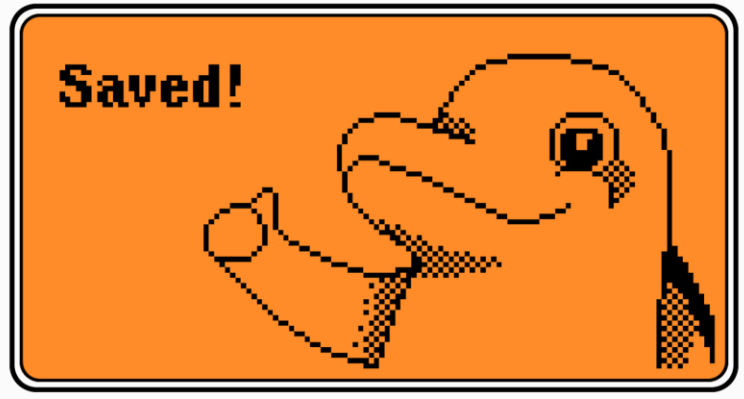




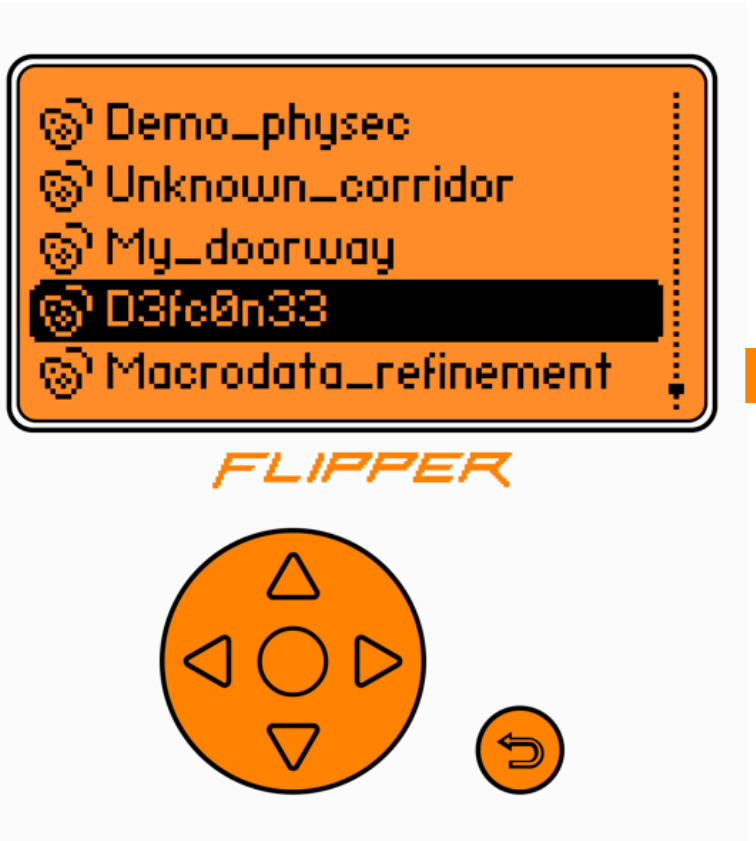


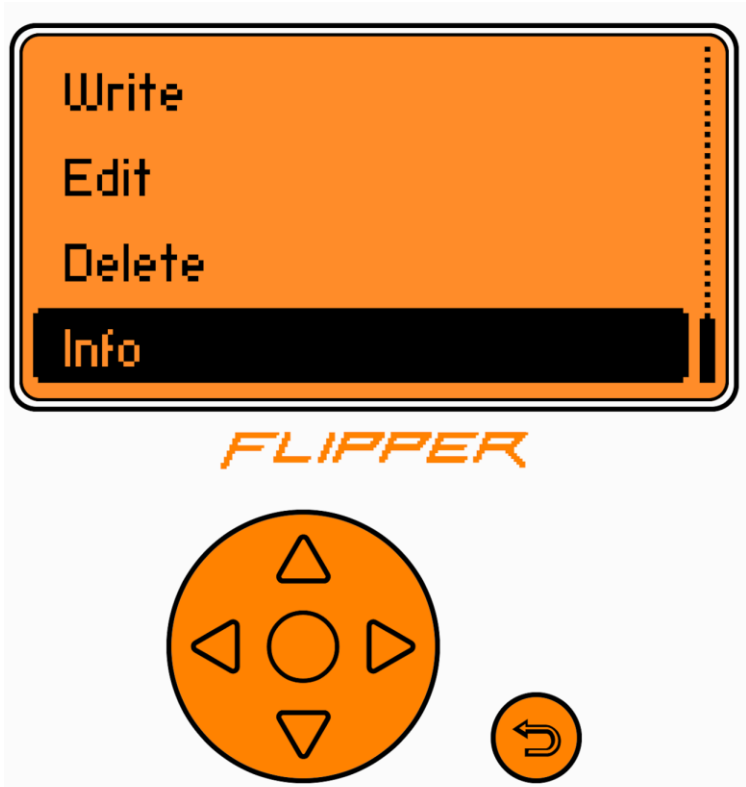
Flipper Zero – Saving Card

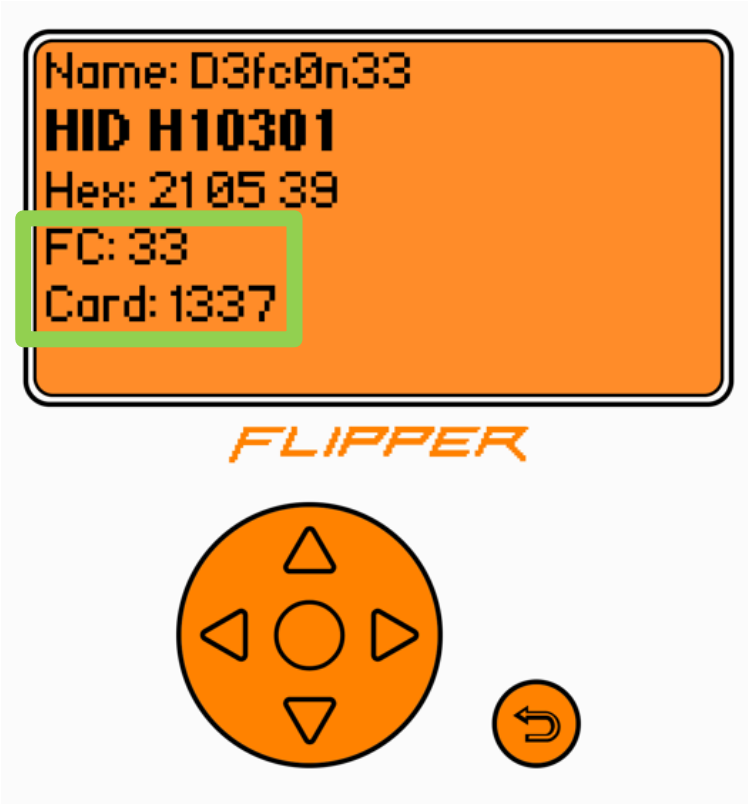




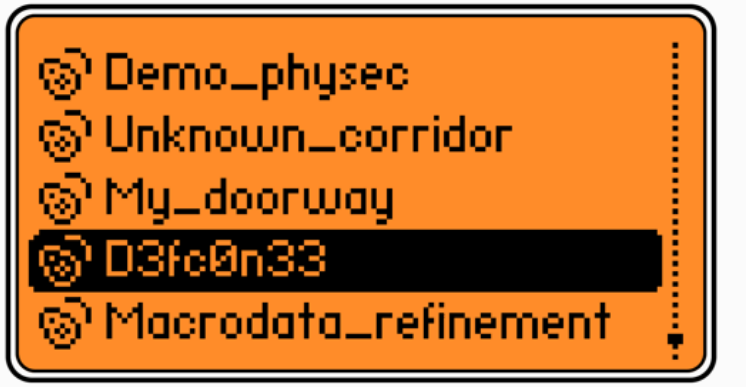
Flipper Zero – Reading Card Info

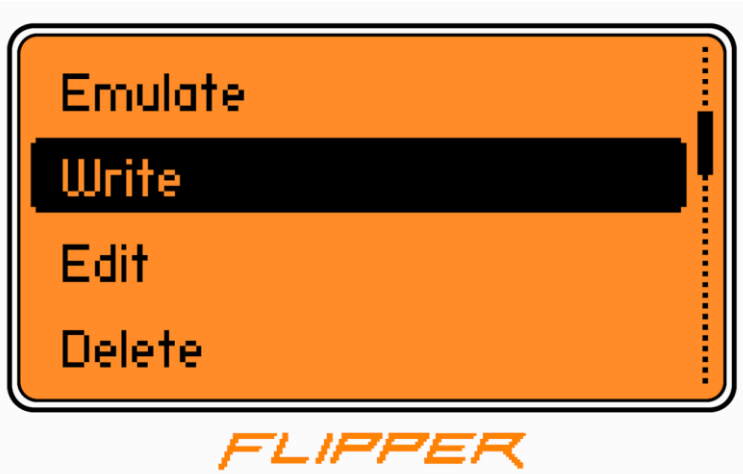


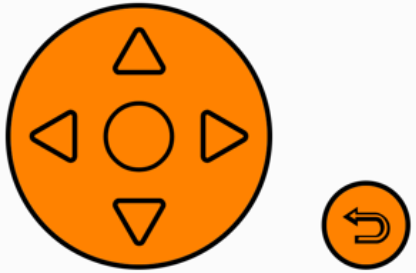


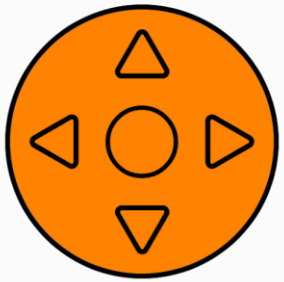


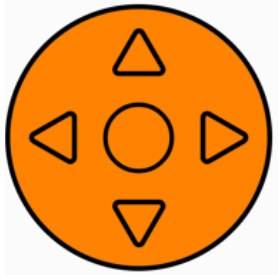
Flipper Zero – Writing Card To Blank Badge



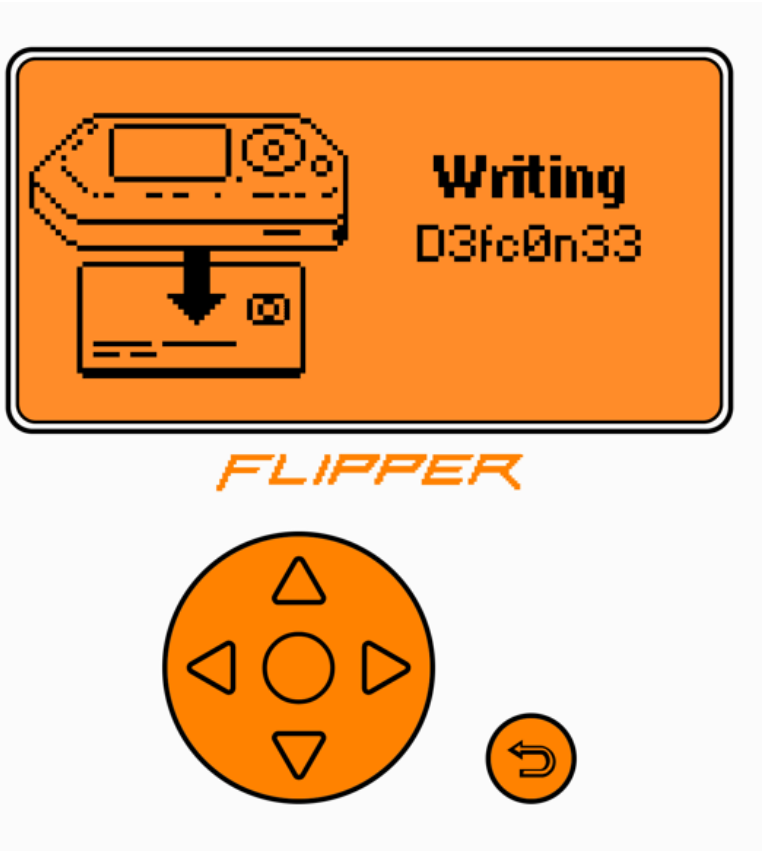


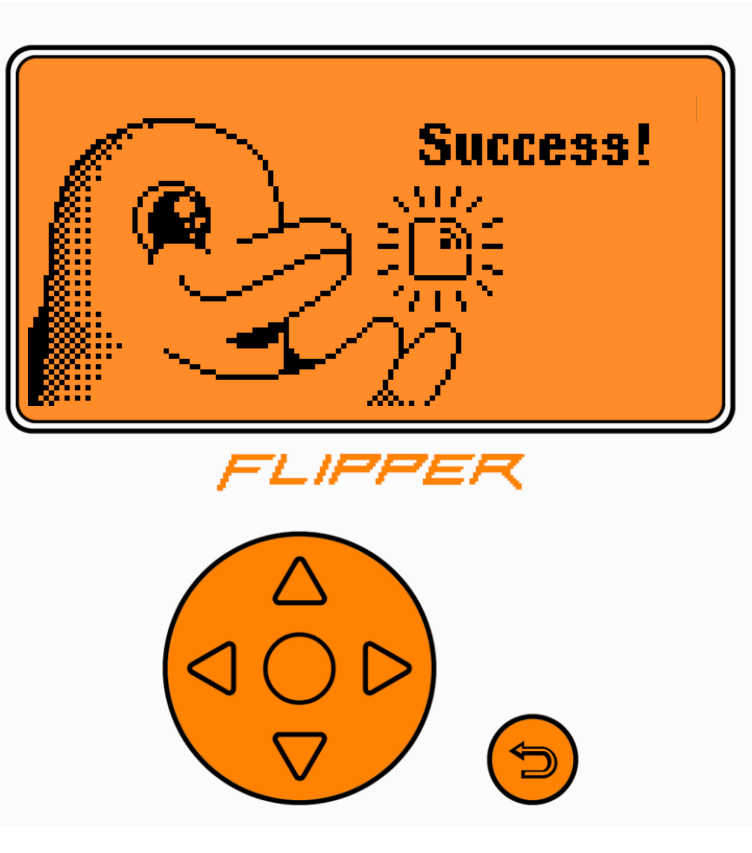






Flipper Zero – Writing Card To Blank Badge





And you're in!


!
LUMON
hello, my name is
MARK SCOUT SVR'D ACCESS
employee code
08-927
signature

HID SE/SEOS Attacks

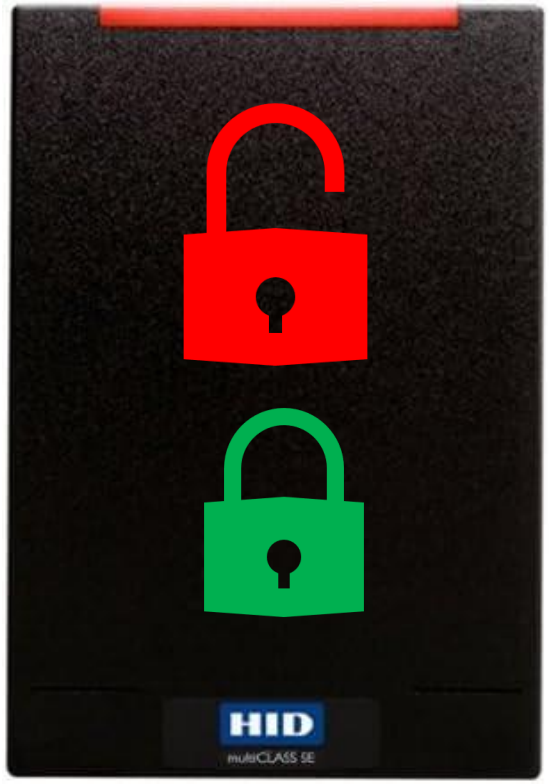
Stealthy Attacks!

HID Reader Protocols

Traditional HID

125Khz (Unencrypted)
~~13.56hz (Encrypted)~~

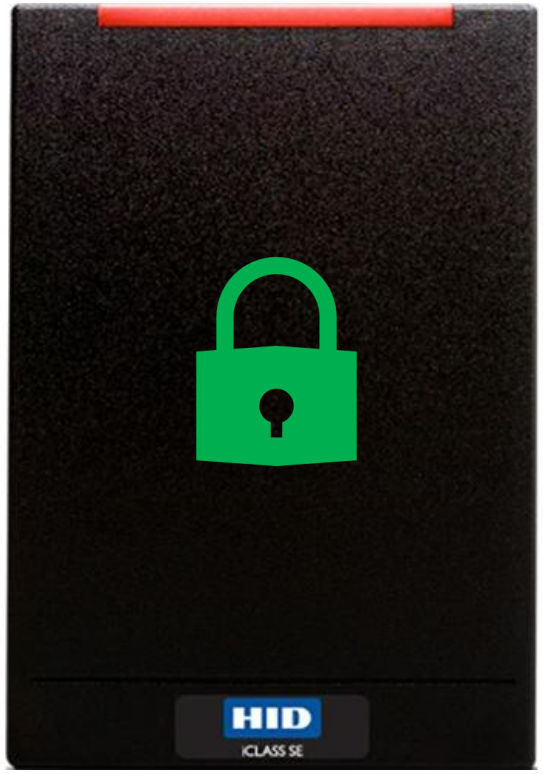
VS.



HID multiCLASS SE

125Khz (Unencrypted)
13.56hz (Encrypted)

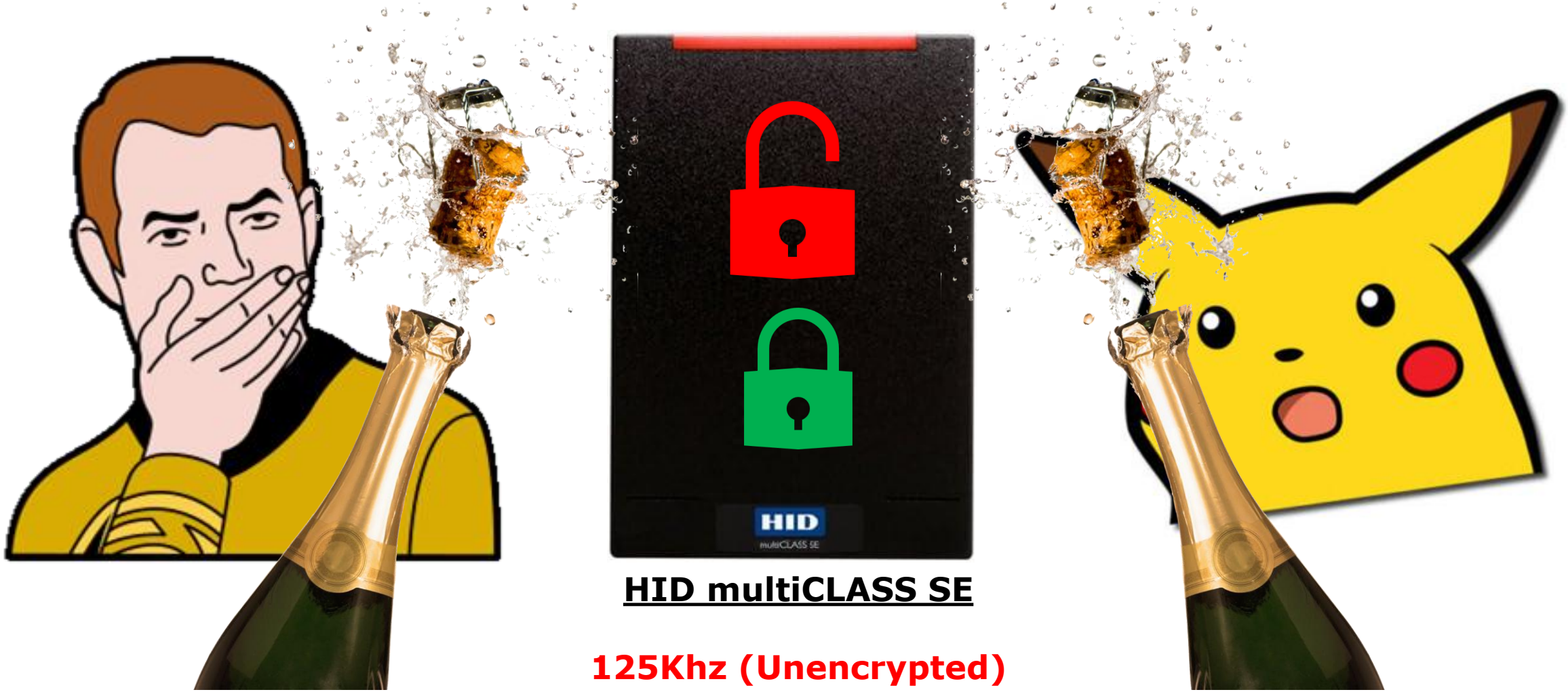
VS.



HID iCLASS SE

~~125Khz (Unencrypted)~~
13.56hz (Encrypted)

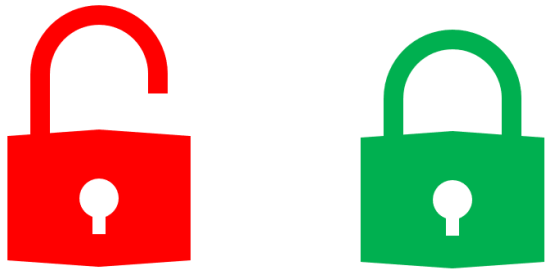
HID multiCLASS SE = Party Time.



HID multiCLASS SE

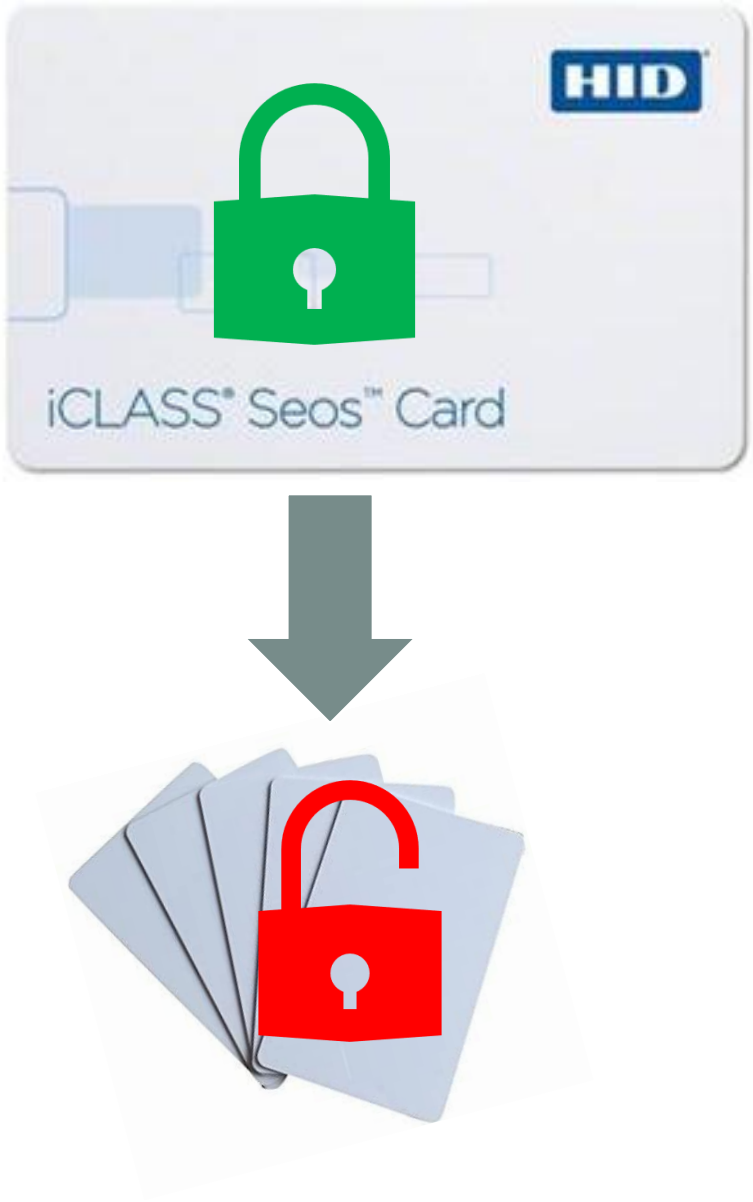
125Khz (Unencrypted)
13.56hz (Encrypted)

HID multiCLASS SE = Party Time.



#1
HID SE/SEOS Downgrade Attack

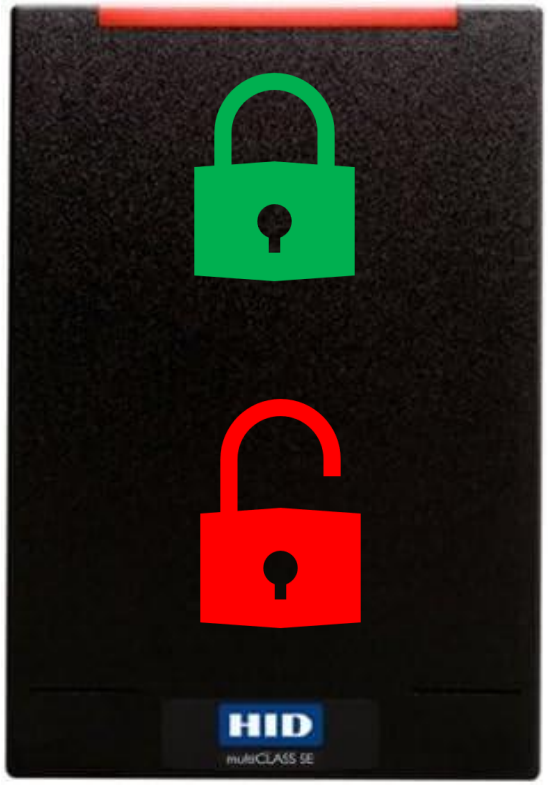
From Encrypted to Unencrypted!



HID SE/SEOS Downgrade Attack

FC = 208 | Card No. = 16398

FC = 208 | Card No. = 16398

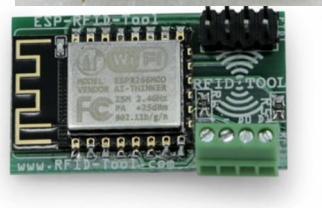


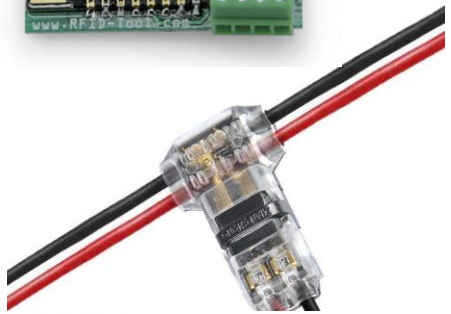
HID multiCLASS SE

Downgrade Attack Build

Downgrade Attack BOM (Build of Materials):

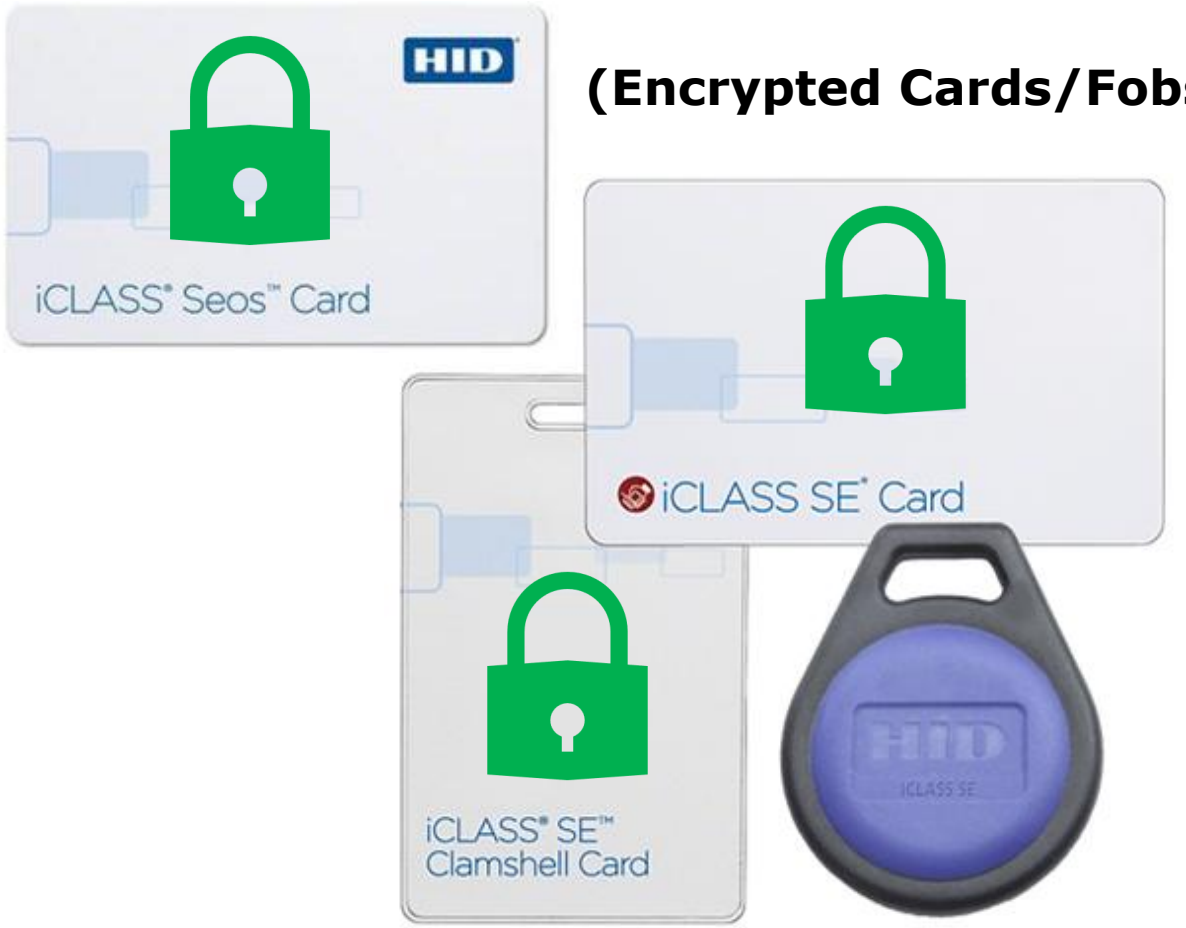
- **HID RP40** (multiclass SE) or **R40** (iCLASS SE)
- ESP RFID Tool OR ESPKey
- 3M Wall Hanging Strips
- 1x 9V 500mAh Rechargeable Battery
- 1x T Tap Connector
- Bread Board Jumper Wires
- 22AWG electrical wire
- Officemate Super Storage Supply Clipboard Case





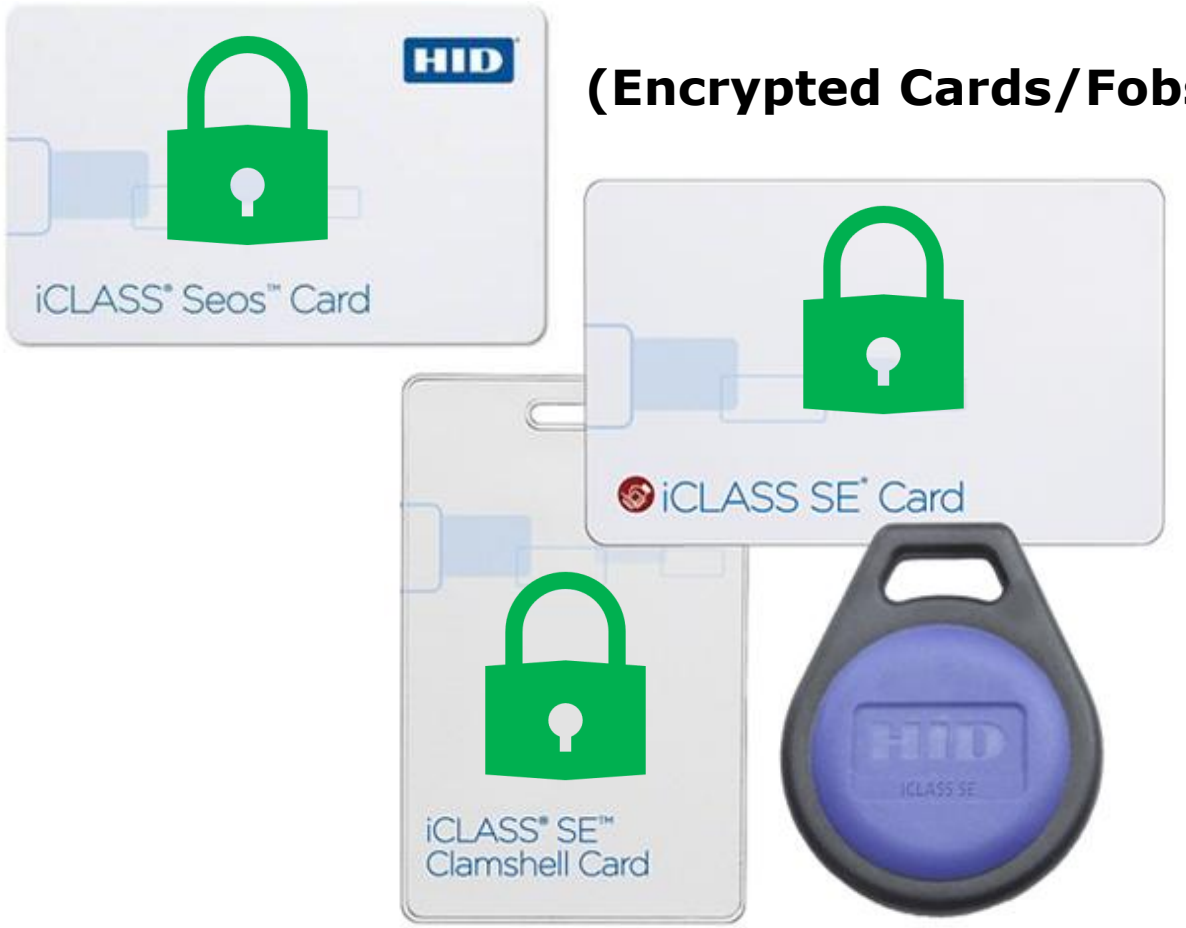
Full Clipboard Cloning build tutorial guide:
http://www.github.com/sh0ckSec/ClipboardCloner

HID SE/SEOS Downgrade Attack – Part 1

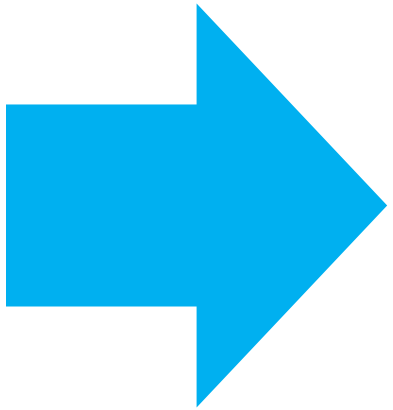


(Encrypted Cards/Fobs)

HID SE/SEOS Downgrade Attack – Part 1



(Encrypted Cards/Fobs)



HID SE/SEOS Downgrade Attack – Part 2

```
/Loot.txt
-----
26 bit card,18 bit preamble,Binary:00000010000000001 01100101101000000000011100 HEX:200596801C
```

1. Copy the second half of the binary data:

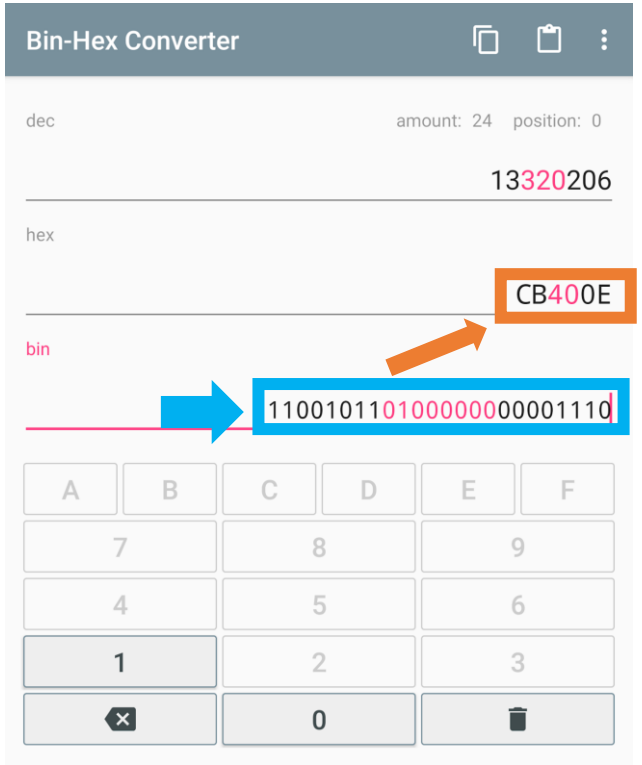
   01100101101000000000011100

2. REMOVE the leading and trailing parity bits:

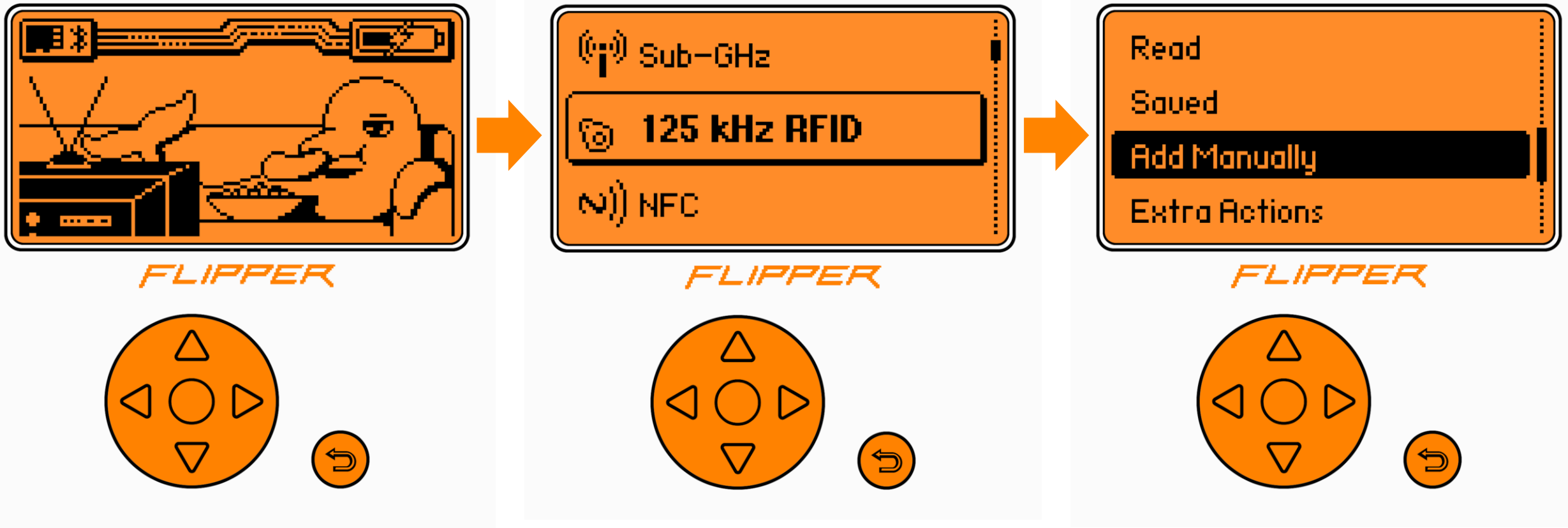
   ~~0~~ **110010110100000000001110** ~~0~~

3. Copy this and convert into HEX using a Bin-HEX Converter

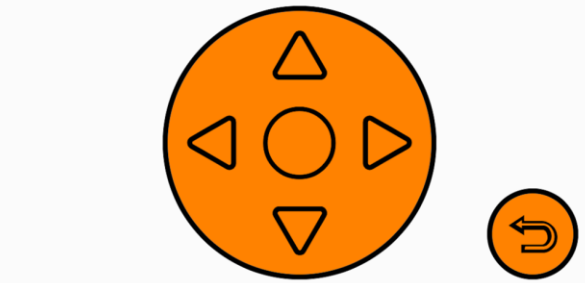
110010110100000000001110 = CB 40 0E

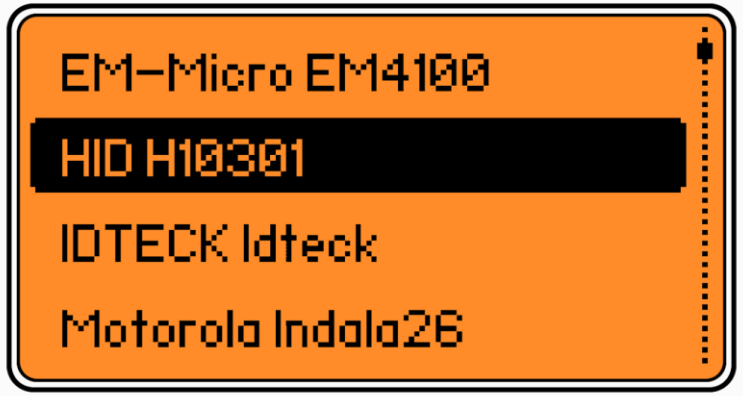


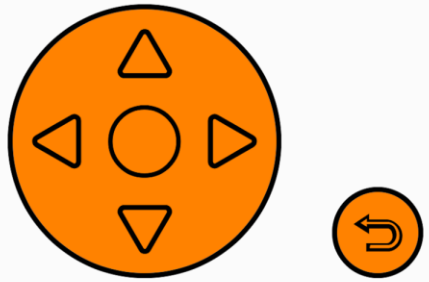
Flipper Zero – Downgrade Attack

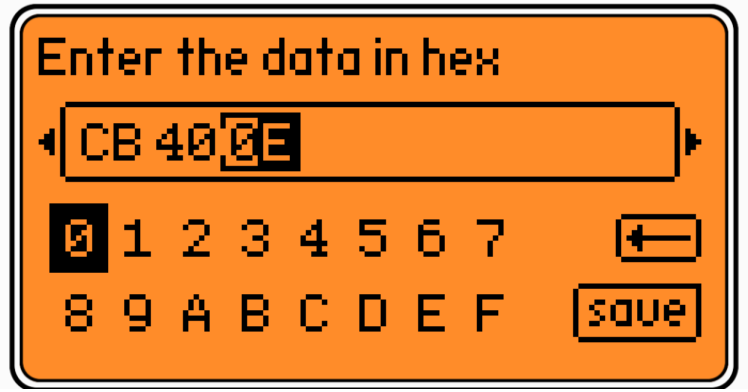


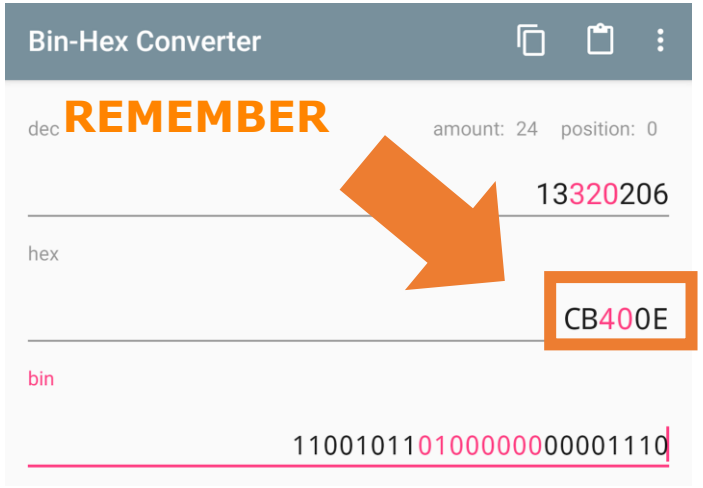
Flipper Zero – Downgrade Attack



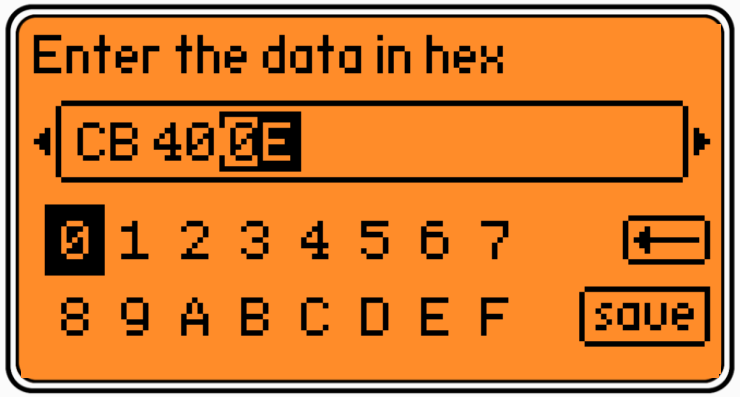


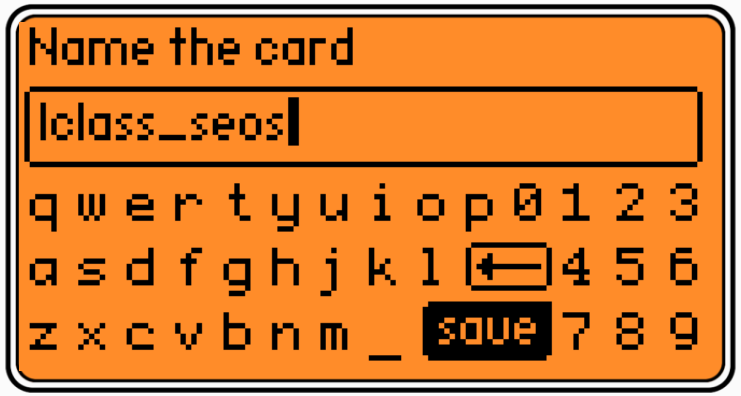


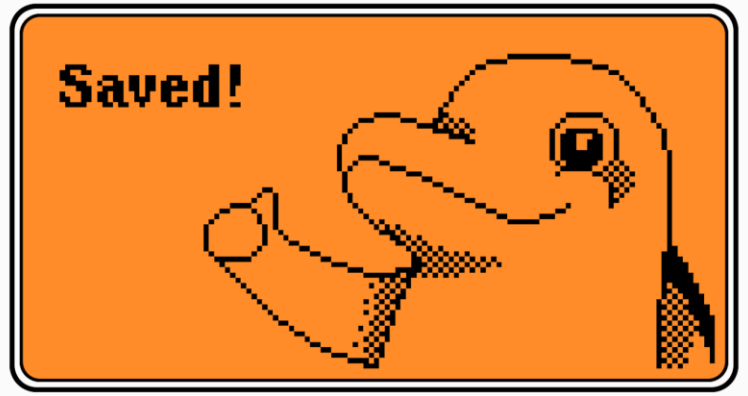




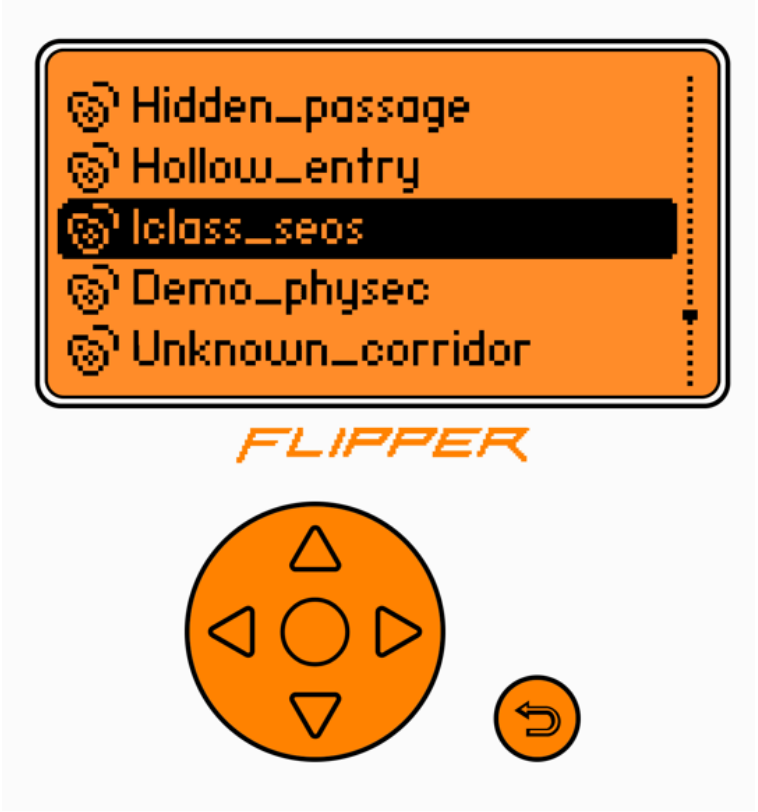
Flipper Zero – Saving Downgraded Card

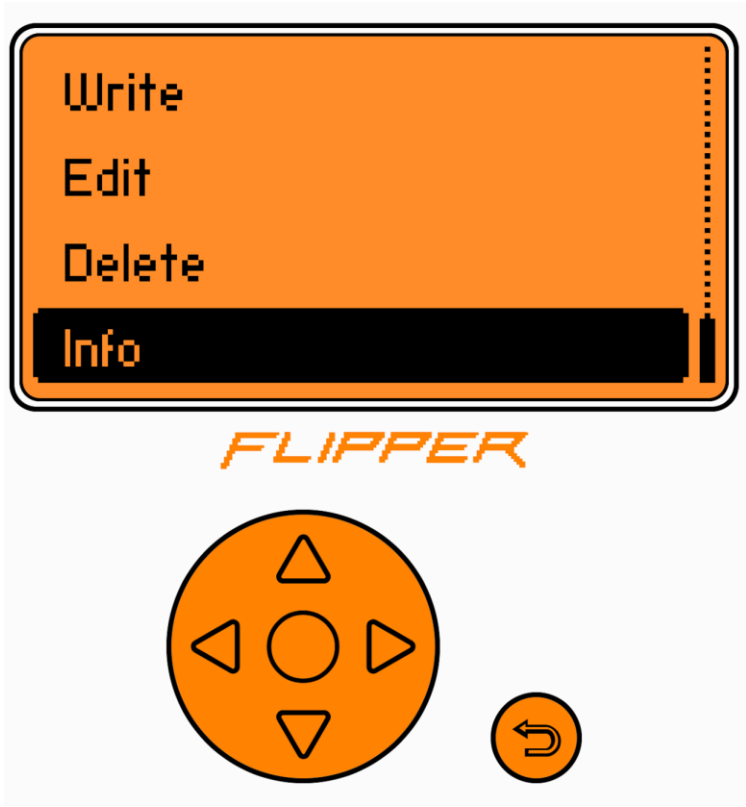


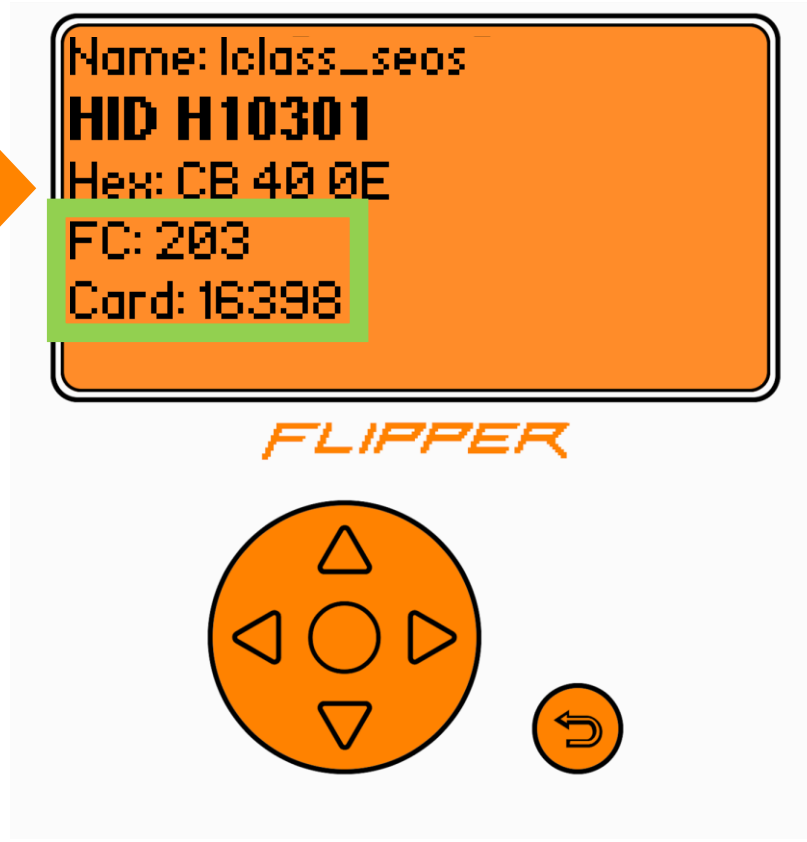




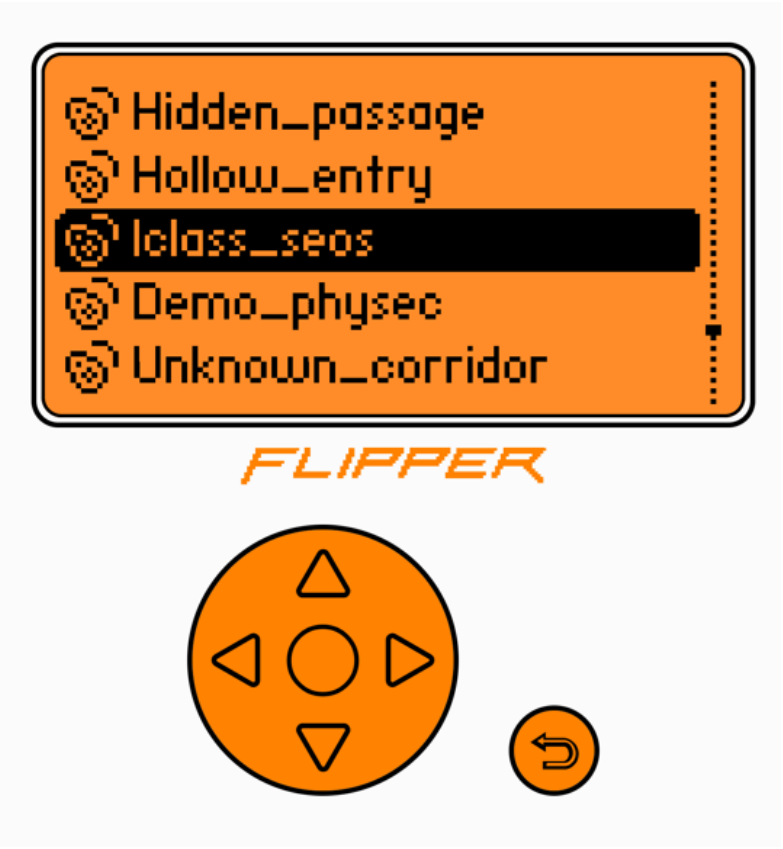
Flipper Zero – Reading Card Info

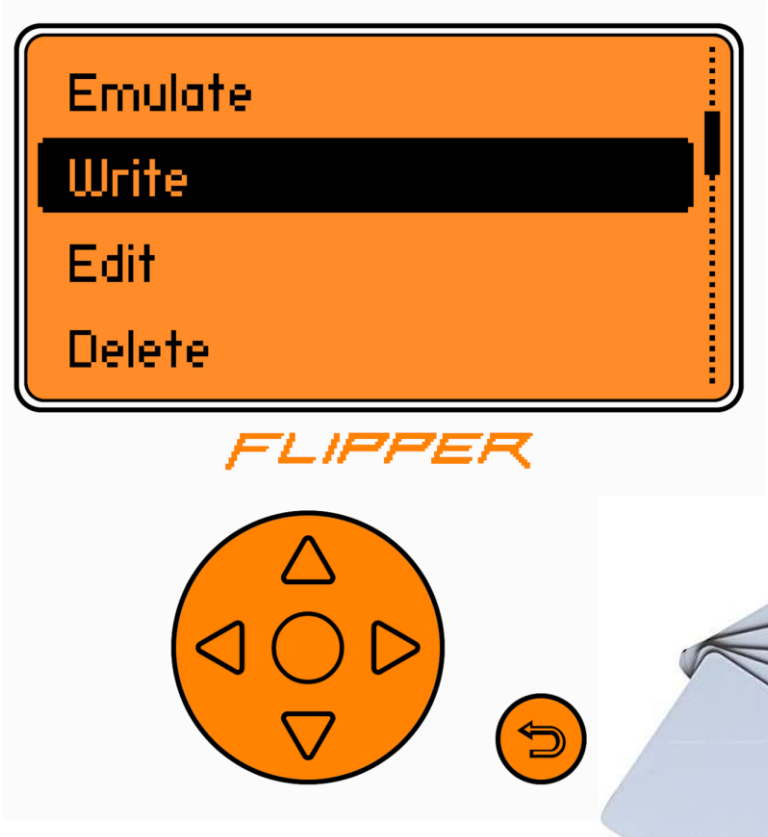


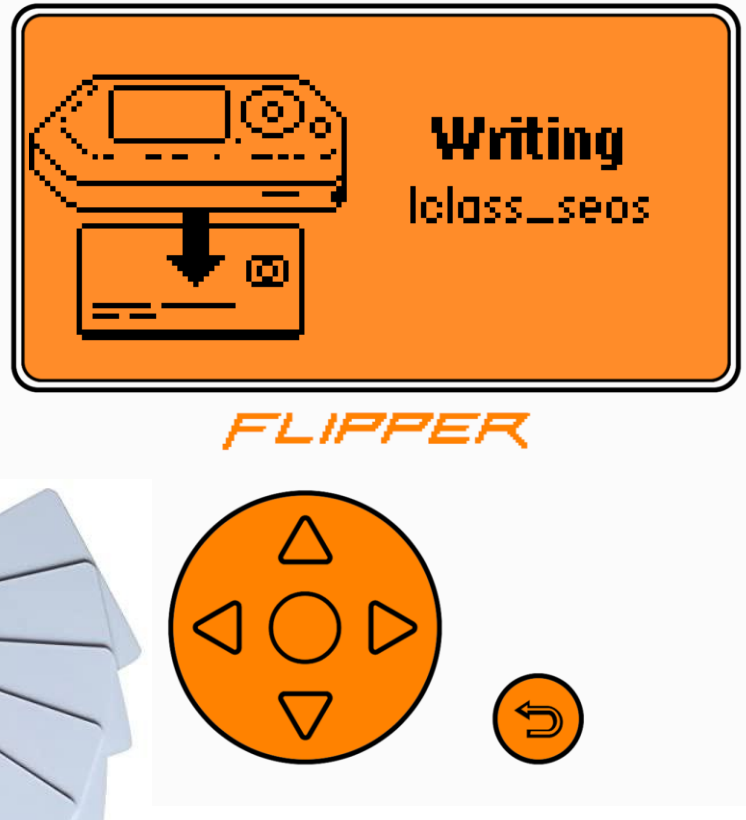




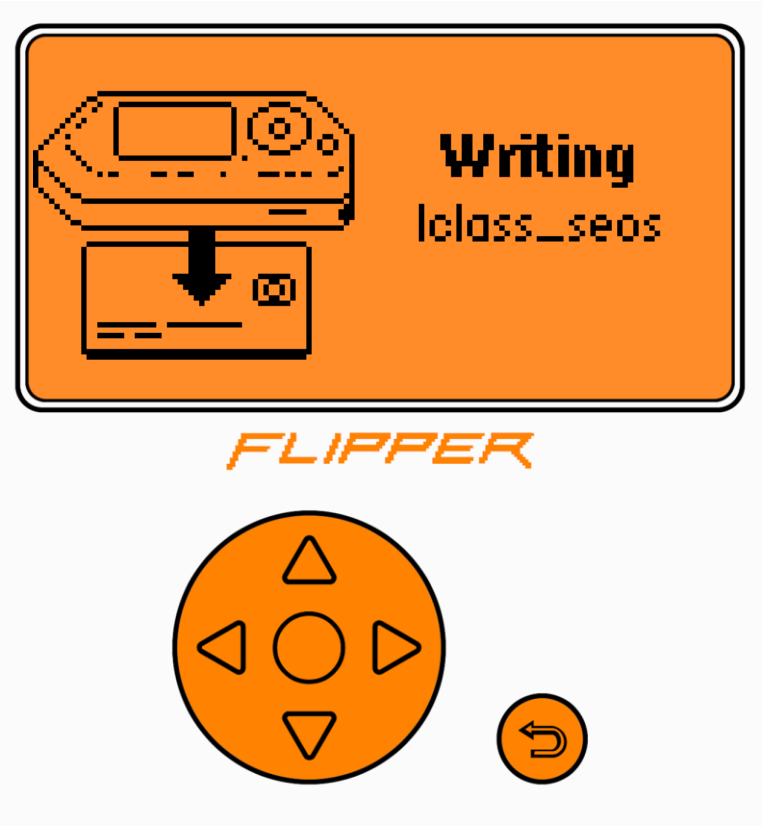
Flipper Zero – Writing Card To Low Freq Badge



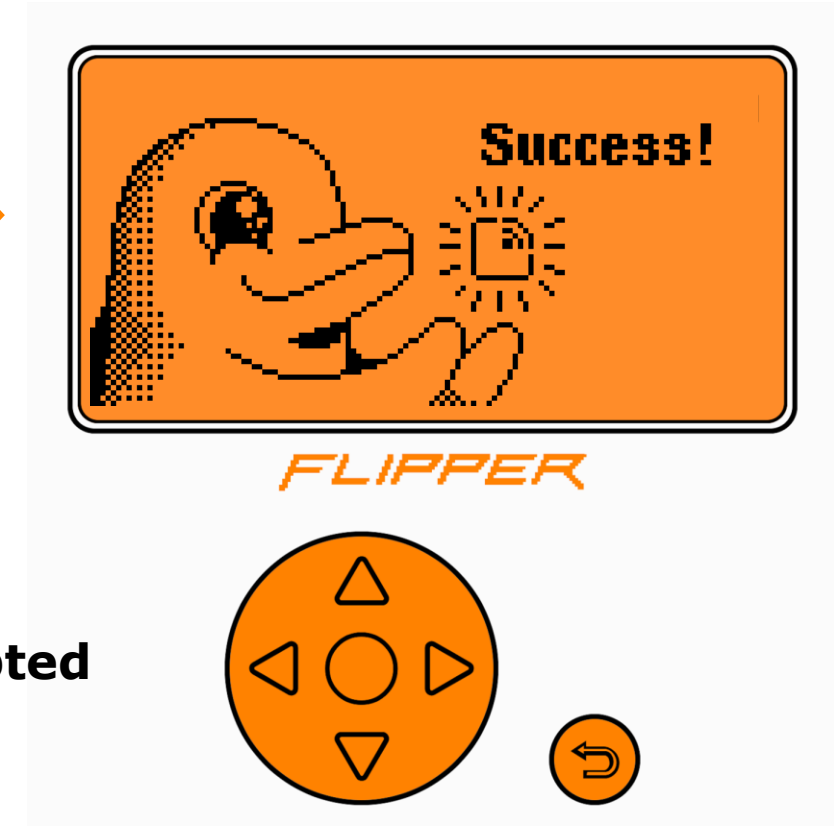




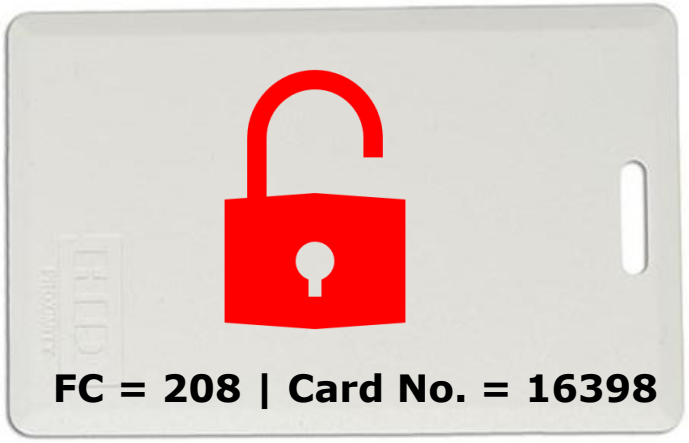
Flipper Zero – Downgrade Complete!



Low Frequency/Non-Encrypted
TM5577 Blank cards



Flipper Zero – Downgrade Attack Complete!



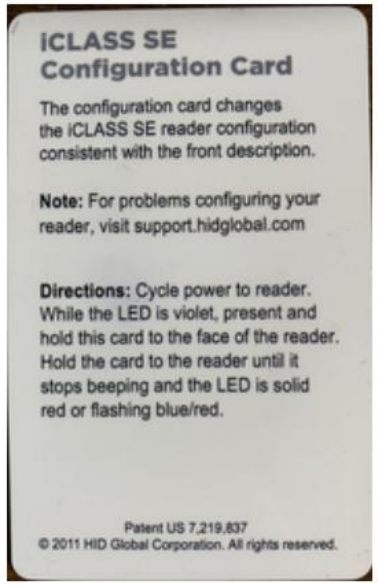
Present the Low Frequency card back to an

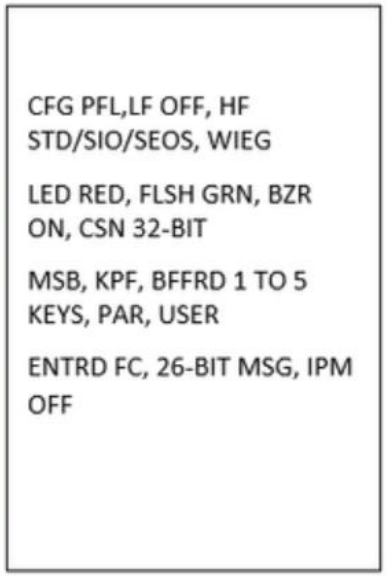
iCLASS multiclass SE reader ONLY!

Mitigations

1. Disable Low-Frequency with iCLASS configuration cards (may require power cycle of each unit).

2. Replace all readers to iClass SE readers, get rid of older multiCLASS readers.





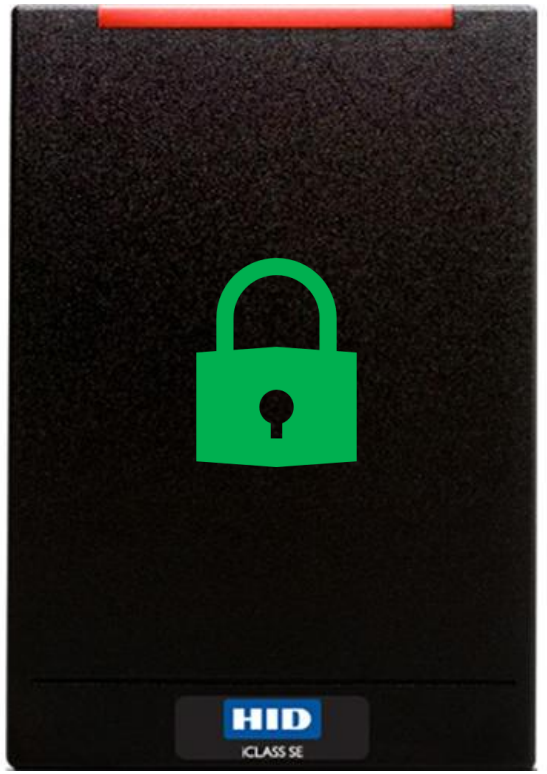
Source: https://tinyurl.com/bdh89zcp

#2
HID SE/SEOS Legacy Attack

Clone using an i-CopyX and an iCS card!

HID SE/SEOS Legacy Attack

- iClass SE/SEOS ONLY
- Downgrade Attack won't work because it can't read unencrypted cards
- Cannot copy SE cards 1:1



HID iCLASS SE

~~125Khz (Unencrypted)~~
13.56hz (Encrypted)

HID SE/SEOS Legacy Attack – iCS Cards

Vulnerable to iCS cards and iCS Decoder

"The iCS Decoder **will only work** for target systems that are configured to **accept legacy cards**. **This is the default configuration.**

This technique will not work on all iCLASS SE readers. Coverage is approximately 85%."

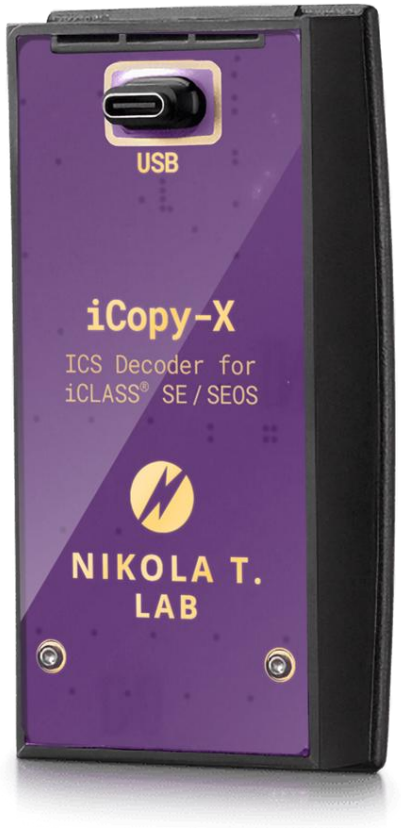
Source: https://icopyx.com/products/iclass-se-seos-decoder

iCopy-X Clipboard Build

Legacy Attack BOM (Build of Materials):

- **iCopy-X (~$400 USD)**
- **ICS Decoder for iCLASS® SE / SEOS (~$460 USD)**
- **iCS cards (~$20 each – one time use!)**
- 3M Wall Hanging Strips
- Officemate Super Storage Supply Clipboard Case

Full Clipboard Cloning build tutorial guide:
http://www.github.com/sh0ckSec/ClipboardCloner

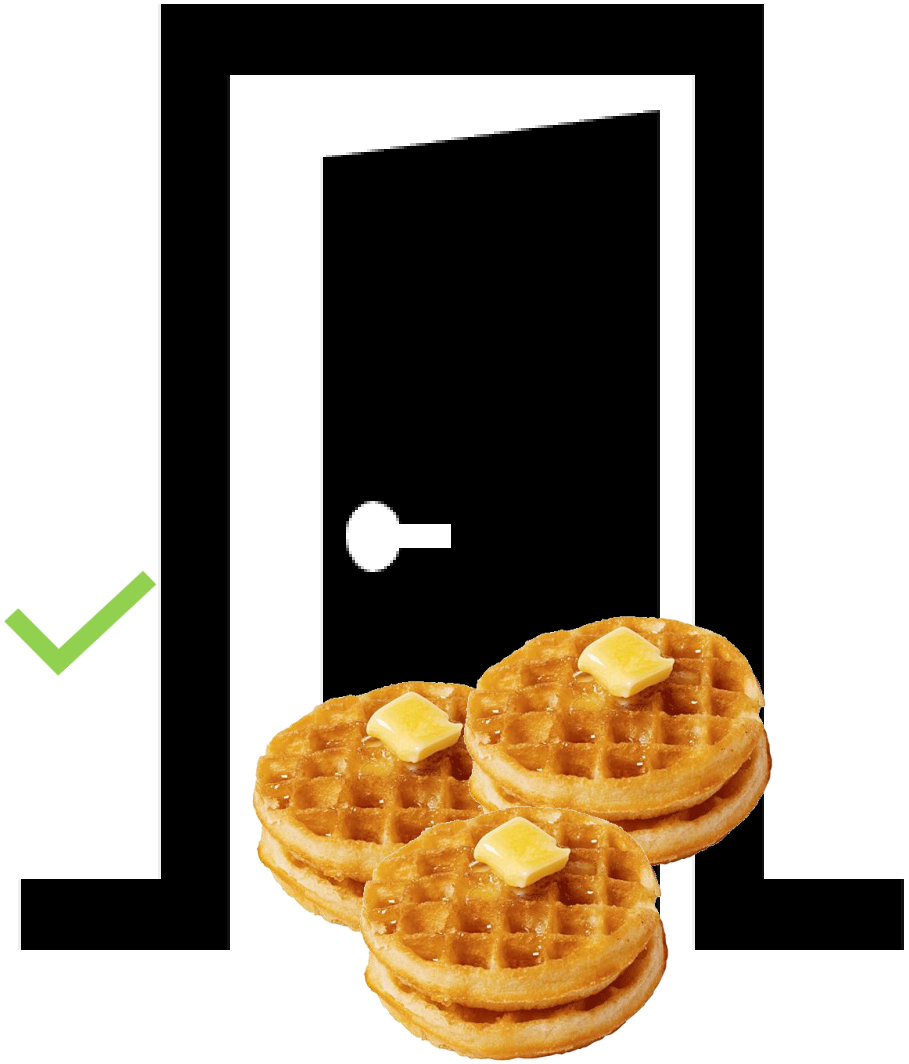


HID SE/SEOS Legacy Attack

HID SE/SEOS Legacy Attack

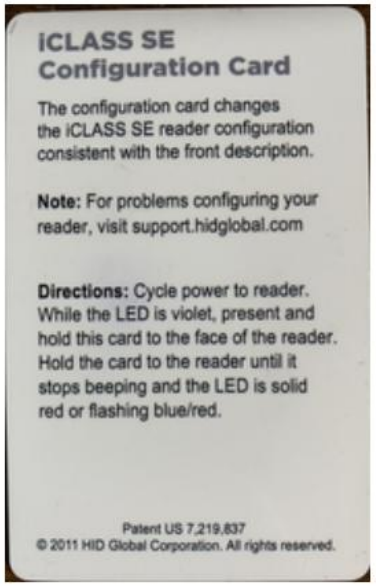
And you're in!

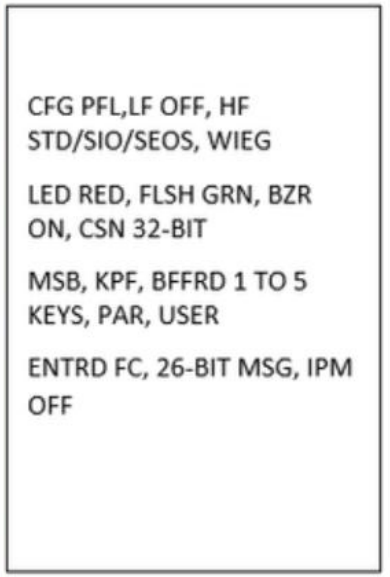

LUMON
hello, my name is
MARK SCOUT SVR'D ACCESS
employee code
08-927
signature



Legacy Attack Mitigations

1. Disable Legacy Card Authentication (the default) with a configuration card.





Source: https://kb.lenels2.com/home/how-do-i-obtain-a-configuration-card-for-my-hid-iclass-or-iclass-se-reader

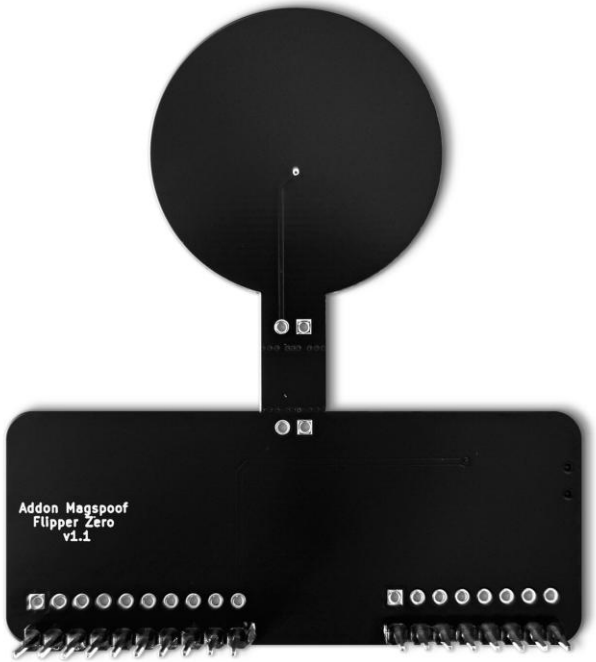
Other Long-Range RFID Readers

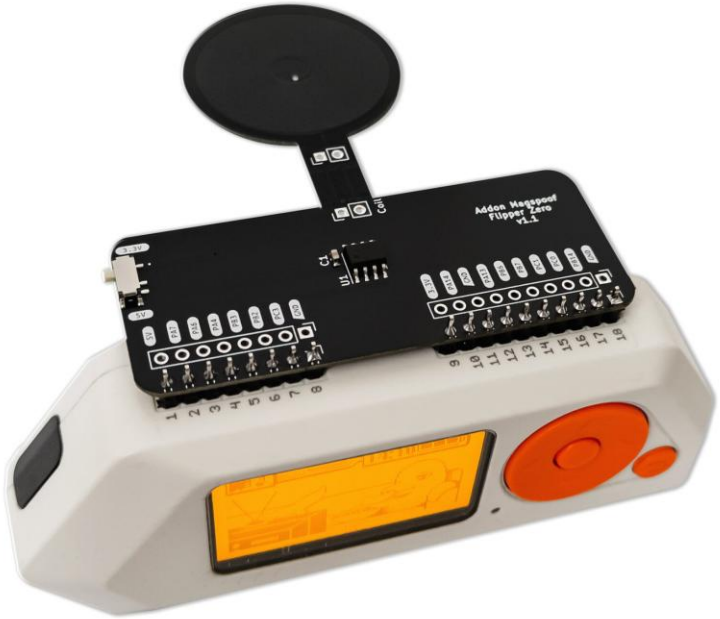
Test out different setups for your target environment!

DL533N XL
LibNFC-Compatible Long-Range RFID Reader / Writer.

ASR-620++
Indala Long-Range Proximity Reader

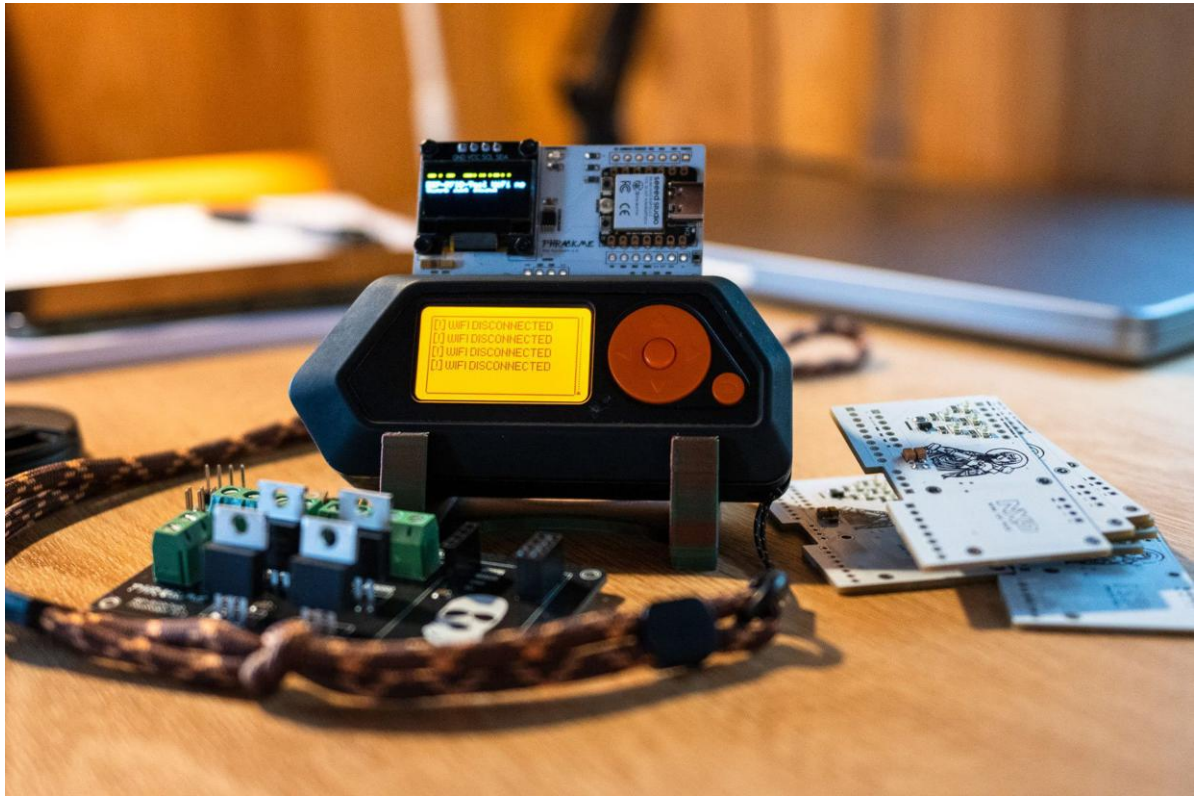
MagSpoof

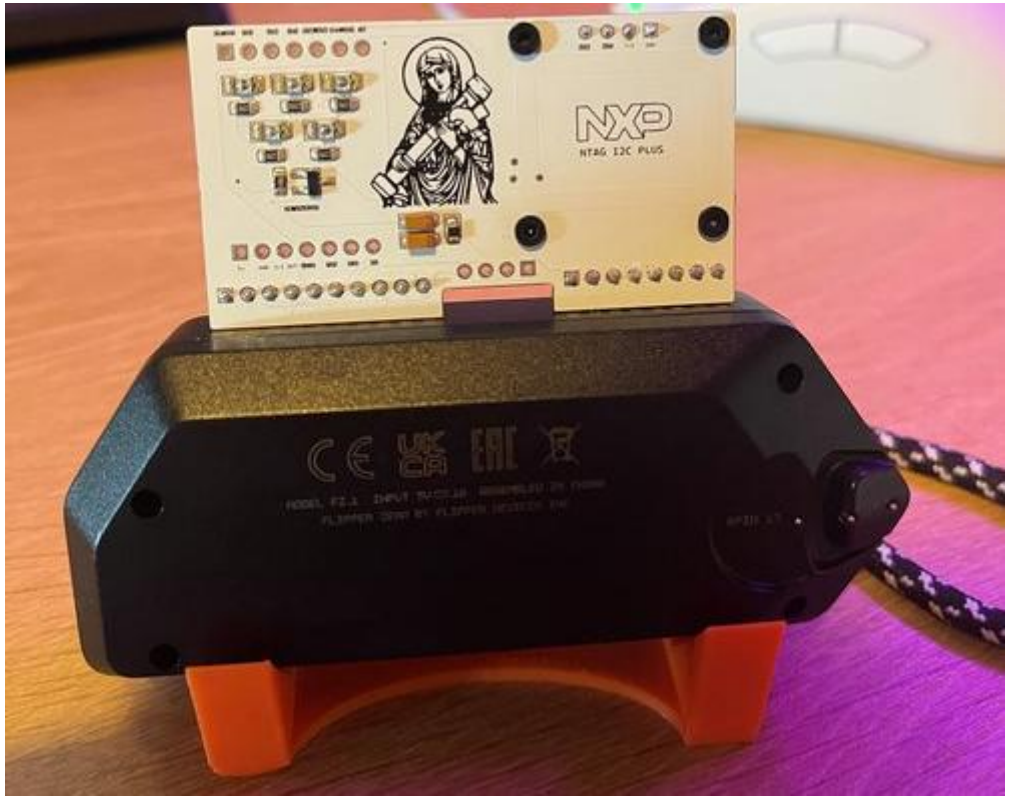




Source: https://electroniccats.com/store/flipper-add-on-magspoof/

RFID Thief by Phrack (Automated workflow!)

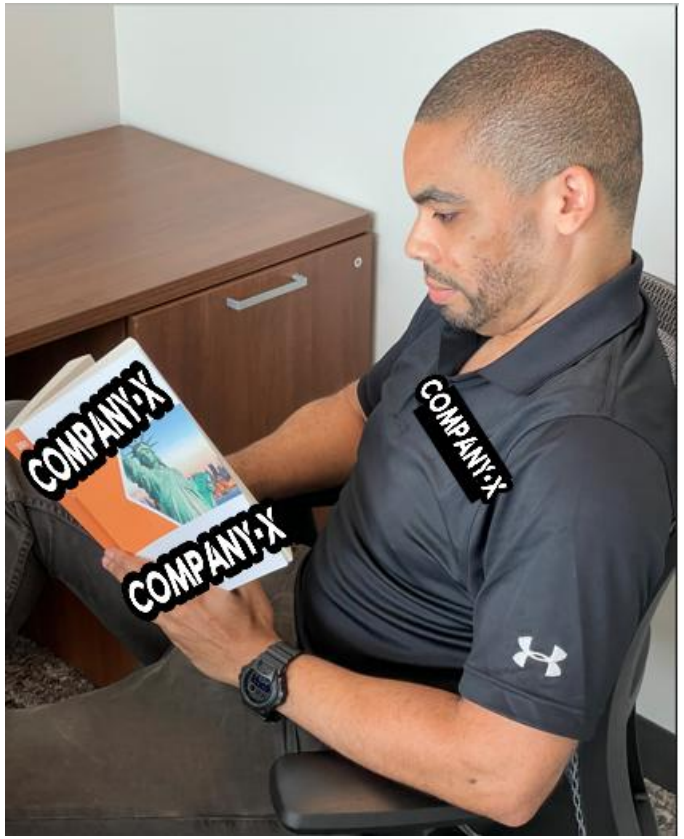




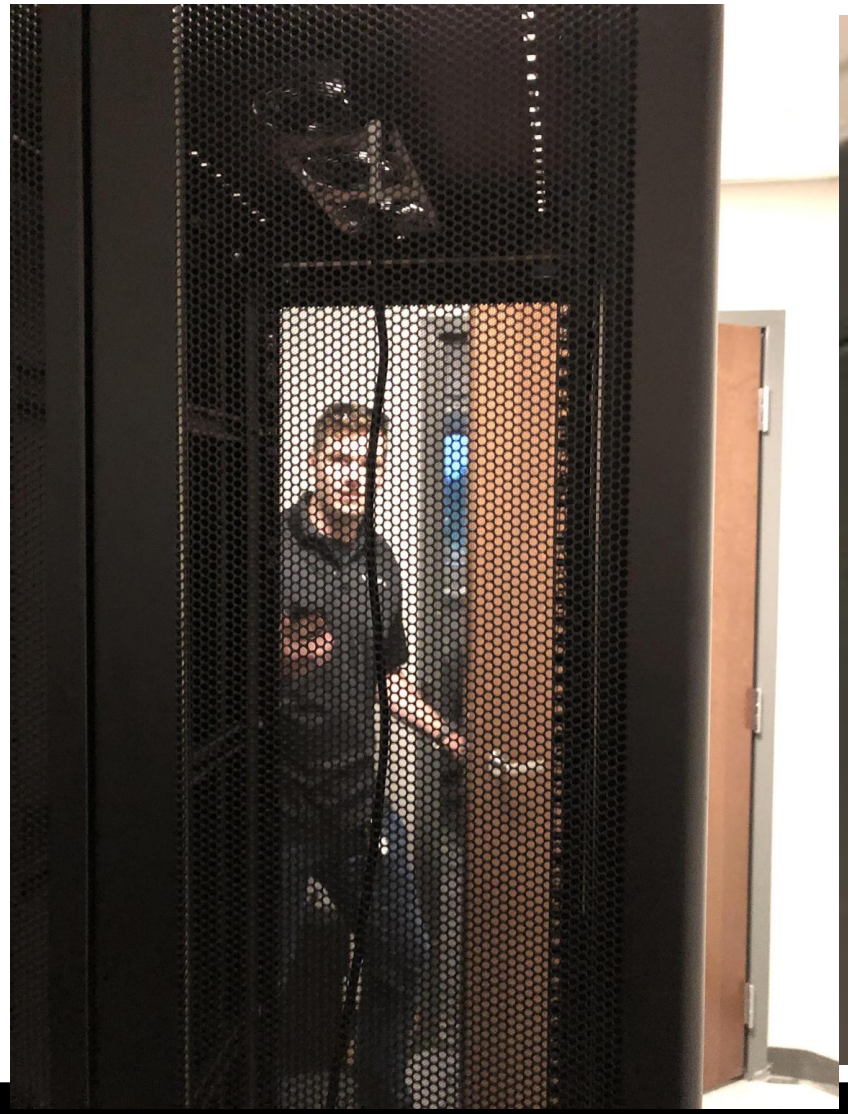
Source: https://www.phrack.me/hardware/2025/02/26/Flipper-Zero-RFIDThief.html

Stories from the Field

AS SEEN IRL...



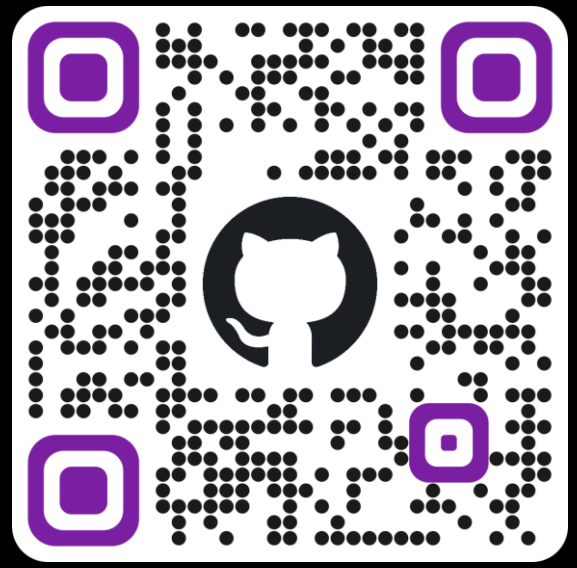
AS SEEN IRL…



References

- Bunsen, Auston. "Examples of every access control bit format." February 2025, https://accessgrid.com/guides/access-control-protocols/examples-of-every-access-control-bit-format
- Farrell, Michael and Boris Hajduk. "AndProx." July 2021, GitHub, https://github.com/AndProx/AndProx
- Harding, Cory. "ESP-RFID-Tool." March 2018, GitHub, https://github.com/rfidtool/ESP-RFID-Tool
- Hughes, Nathan. "Flipper Maker" May 2022, https://flippermaker.github.io
- Kelly, Mike. "Wiegotcha – RFID Thief." January 2017, https://exfil.co/2017/01/17/wiegotcha-rfid-thief/
- Phrack. “Flipper Zero RFID Thief” https://www.phrack.me/hardware/2025/02/26/Flipper-Zero-RFIDThief.html
- Rumble, Rich. "RFID Sniffing Under Your Nose and in Your Face." DerbyCon IX, September 2019, https://www.youtube.com/watch?v=y37j6RDtybQ
- W., Viktor. "Enclosure For Proxmark3 Easy." Thingiverse, September 2018, https://www.thingiverse.com/thing:3123482
- White, Brent and Tim Roberts. "Breaking Into Your Building: A Hacker's Guide to Unauthorized Access." NolaCon 2019, May 2019, https://www.youtube.com/watch?v=eft8PElmQZM

THANK YOU!



@sh0ckSec

github.com/sh0cksec

@_BadCharacters

Badcharacters.io