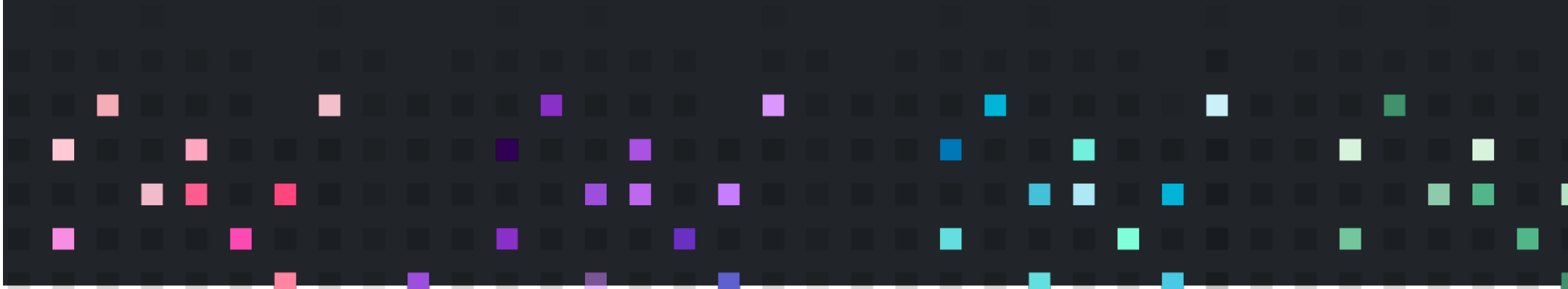
How My DIY RFID Reader Became a Lifesaver

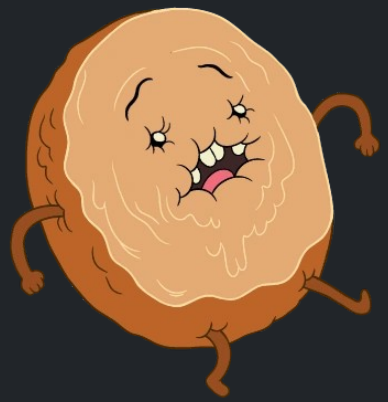
SecretCon 2 | Dale Cook



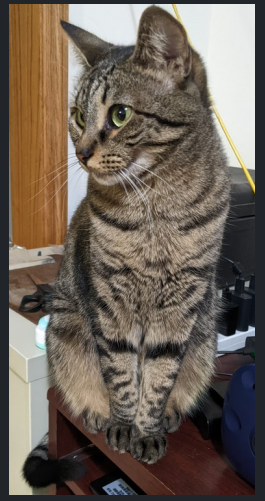
whoami

- D0zer aka Decrazyo
- Penetration tester
  - OSCP, OSCE, OSWE certified
- Exploit developer
  - I’ll use any language but Java
- Electronics hobbyist
  - Not an electrical engineer!

Background



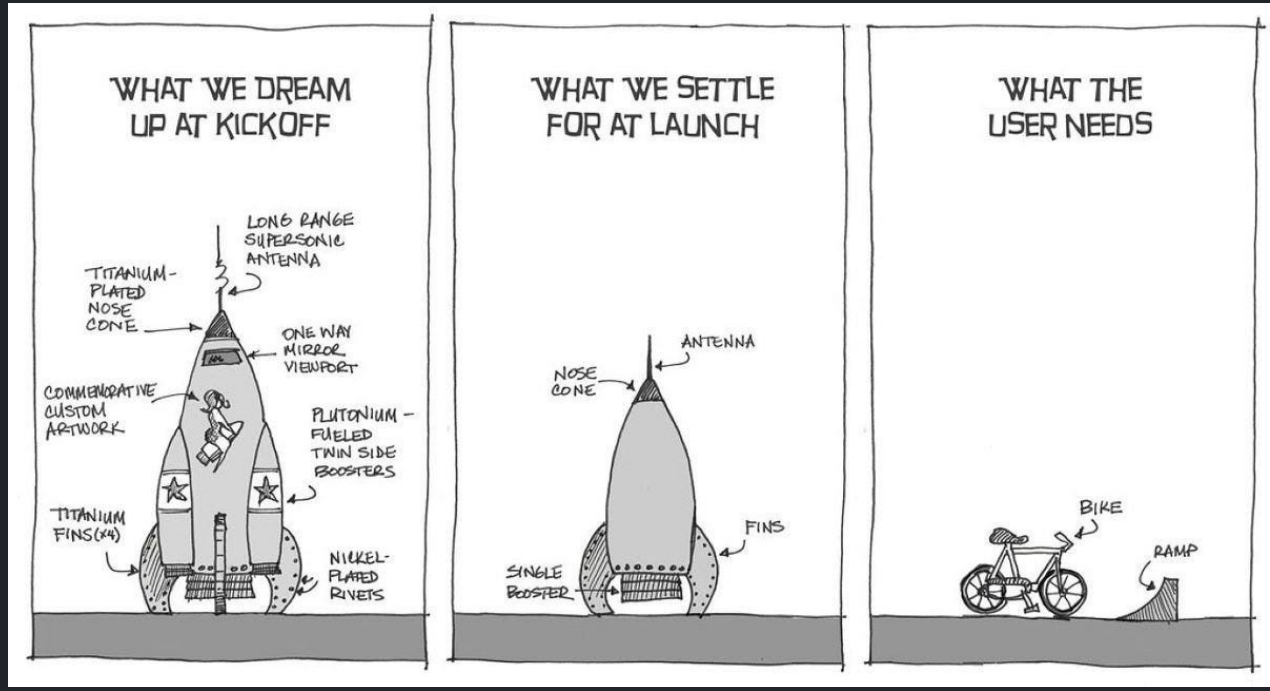
Cinnamon Bun



Huntress Wizard

Background

Background


WHAT WE DREAM UP AT KICKOFF
LONG RANGE SUPERSONIC ANTENNA
TITANIUM-PLATED NOSE CONE
ONE WAY MIRROR VIEWPORT
COMMEMORATIVE CUSTOM ARTWORK
PLUTONIUM-FUELED TWIN SIDE BOOSTERS
TITANIUM FINS (x4)
NICKEL-PLATED RIVETS
WHAT WE SETTLE FOR AT LAUNCH
ANTENNA
NOSE CONE
FINS
SINGLE BOOSTER
WHAT THE USER NEEDS
BIKE
RAMP

Background

Spoiler alert

It didn’t work

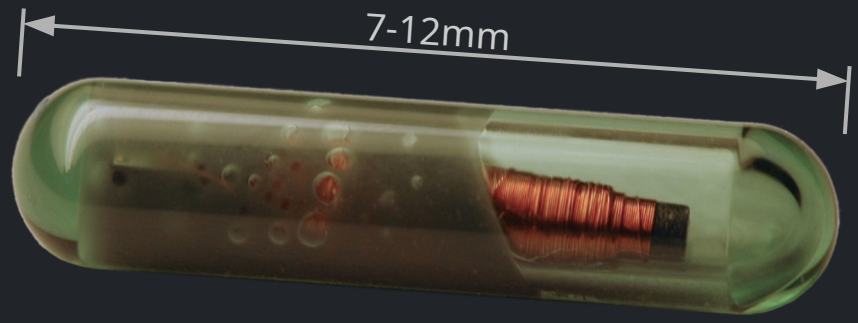
Background

1) RFID is short range

2) Cats are jerks

RFID Tag

- Glass capsule
  - Antenna coil
  - Integrated circuit
    - Non-volatile memory
    - Transmitter logic

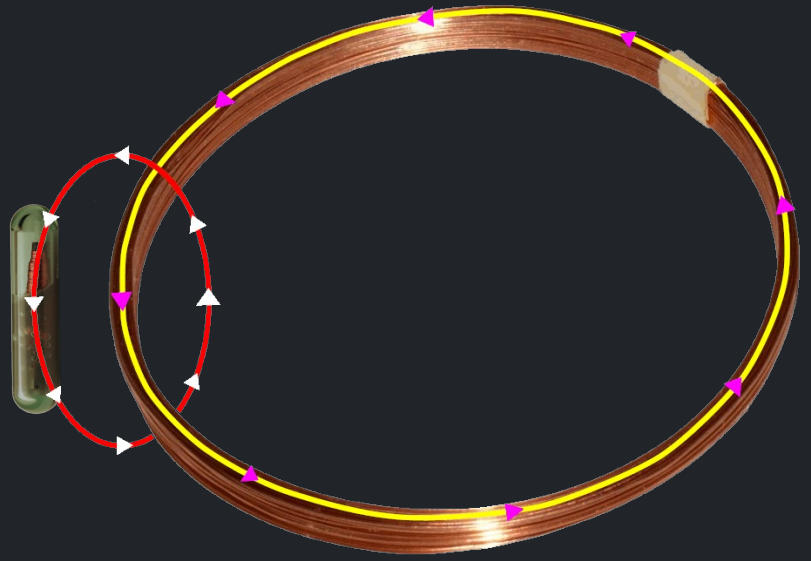


RFID Reader

- Power
- Clock signal
- Communication channel

RFID Reader

- Power
- Clock signal
- Communication channel



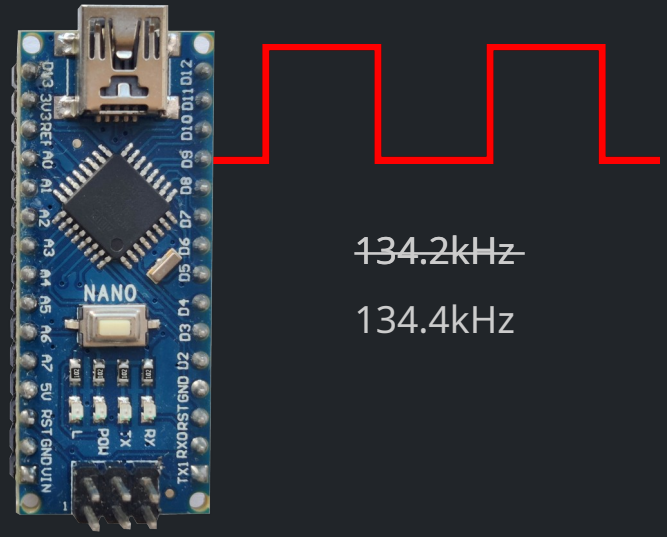
RFID Reader

- Power
- Clock signal
- Communication channel

RFID Reader

- 5V Arduino Nano @ 16MHz

RFID Reader

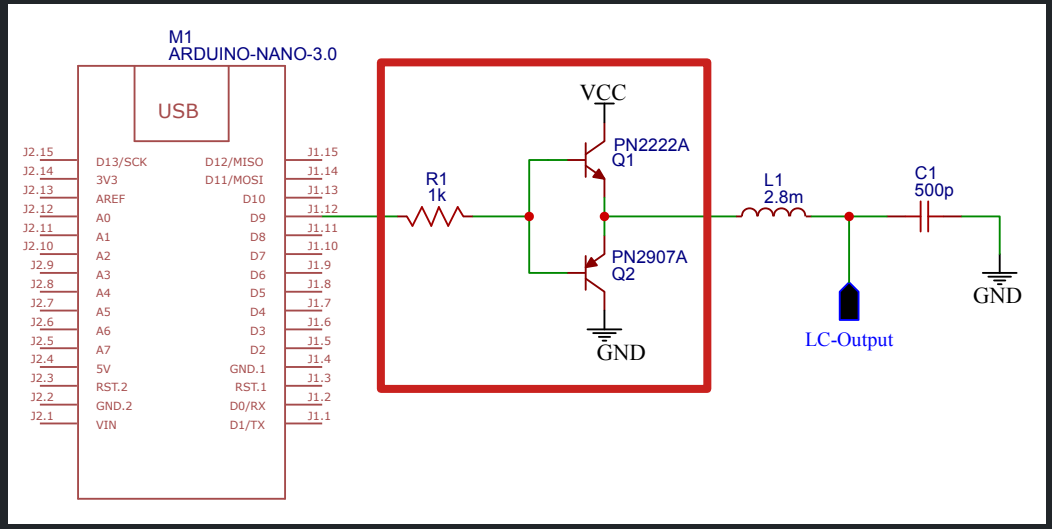


~~134.2kHz~~

134.4kHz

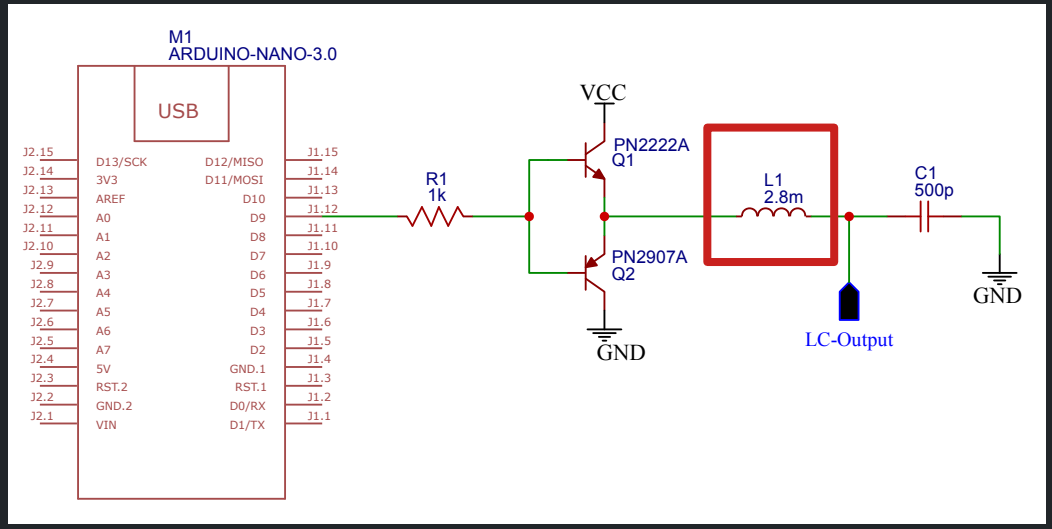
- 5V Arduino Nano @ 16MHz
- Pulse width modulation (PWM)
  - 16-bit timer

RFID Reader



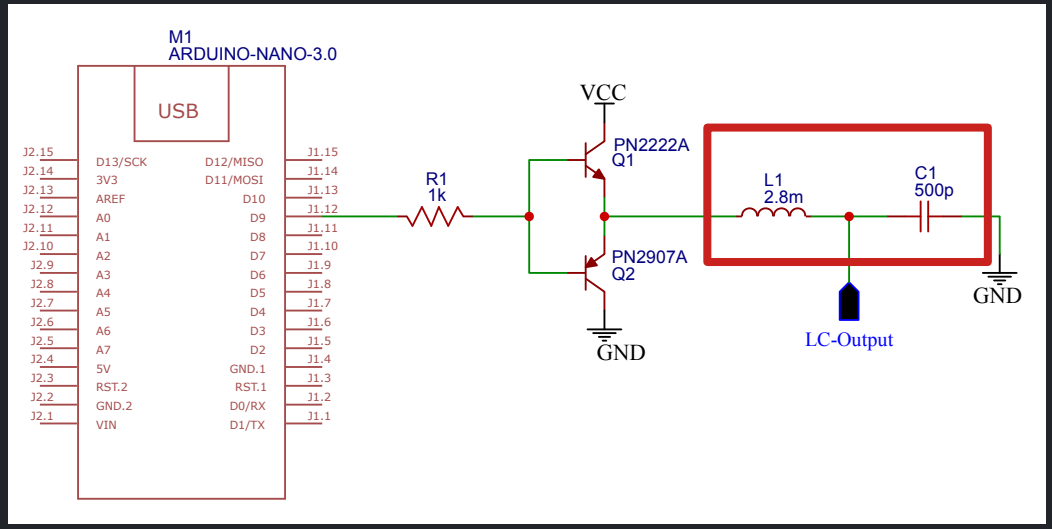
- Push-pull amplifier

RFID Reader



- Push-pull amplifier
- Antenna coil

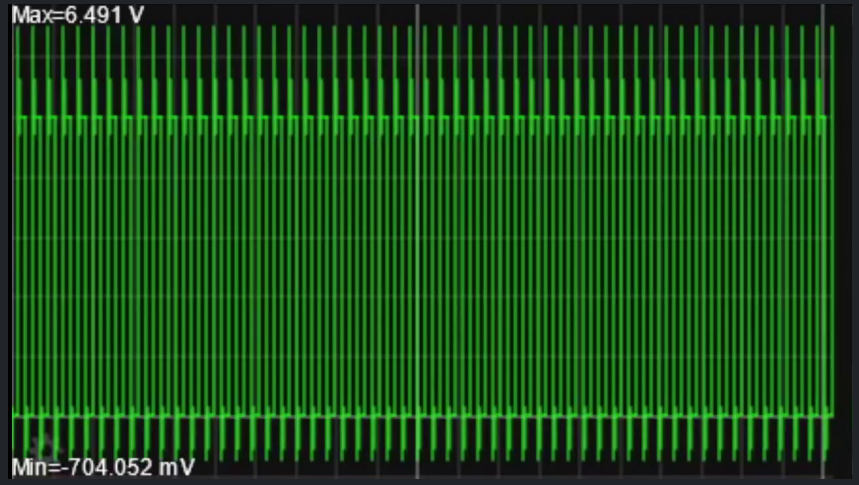
RFID Reader



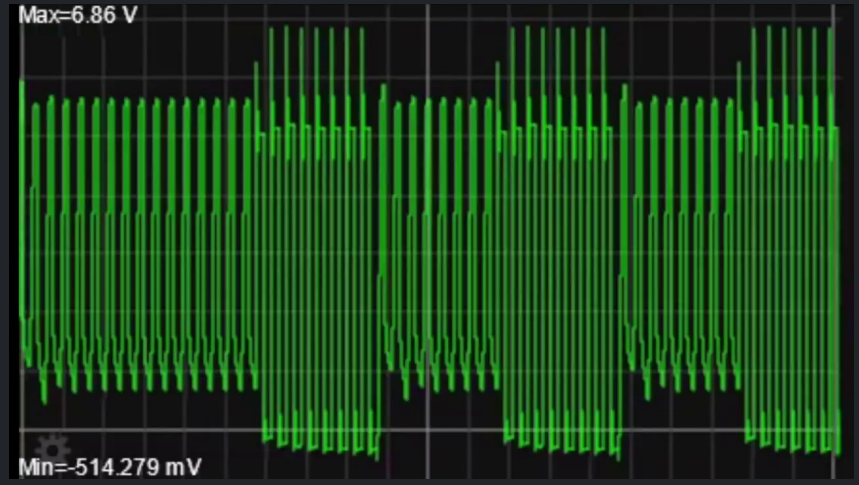
- Push-pull amplifier
- Antenna coil
- LC resonator
  - $f = \frac{1}{2\pi\sqrt{L \times C}}$
  - $134.40\,kHz \approx \frac{1}{2\pi\sqrt{2.8\,mH \times 500\,pF}}$

RFID Reader

Reader antenna

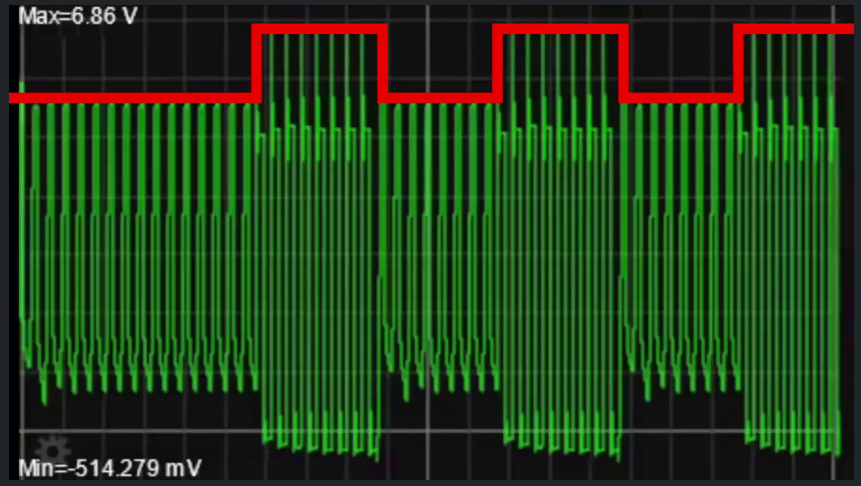


Reader antenna with tag



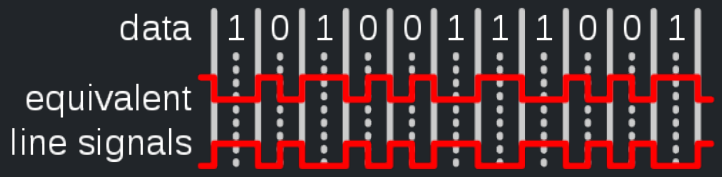
Modulation

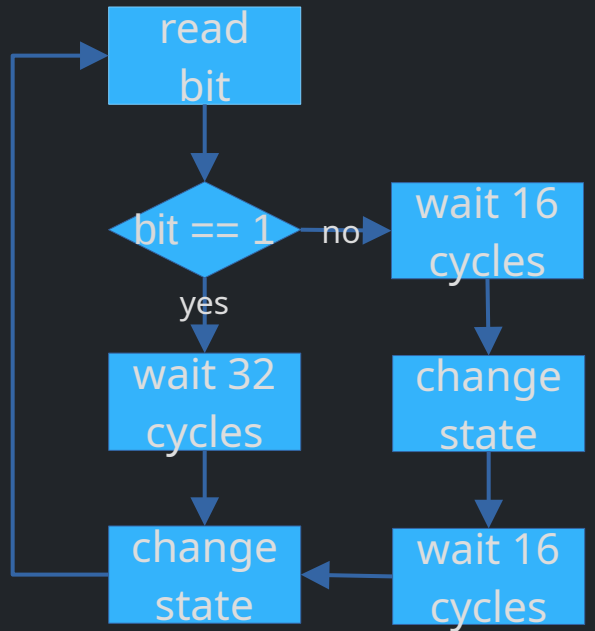
- Amplitude shift keying (ASK)
  - AM radio
  - Digital data



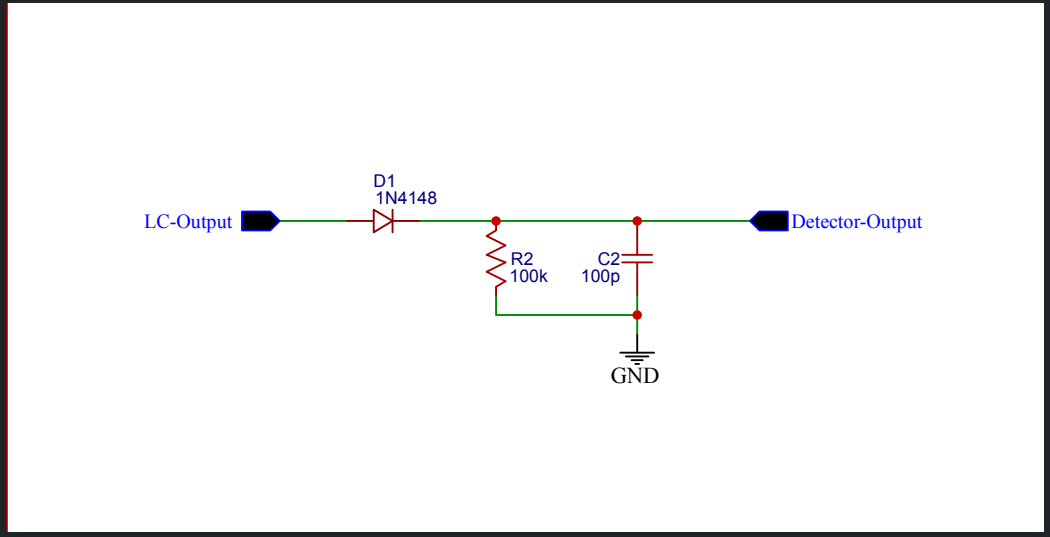
Encoding

- Differential Manchester
- 32 cycle bit period
  - Data signal frequency $8.4\,kHz = \frac{134.4\,kHz}{16}$



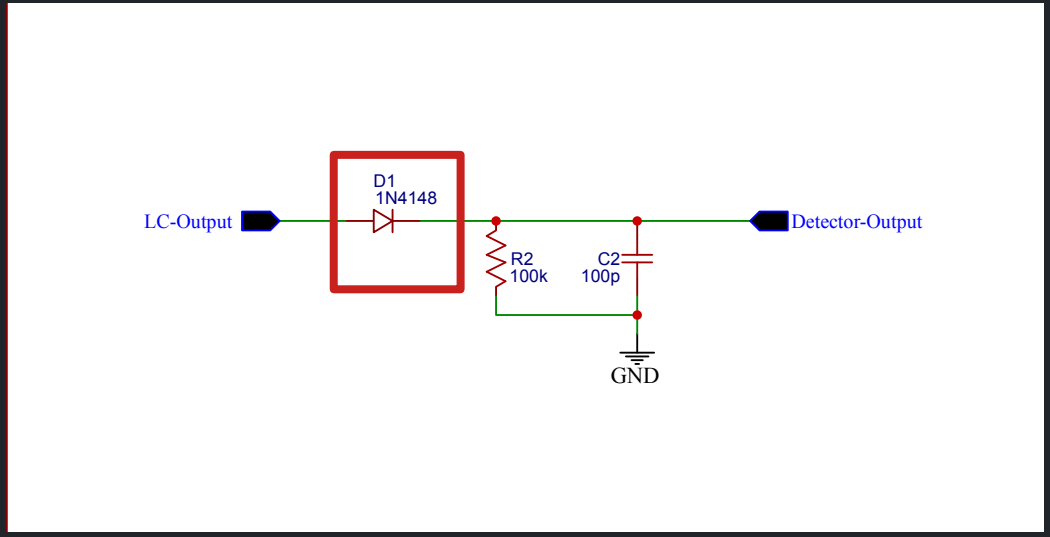


Demodulation



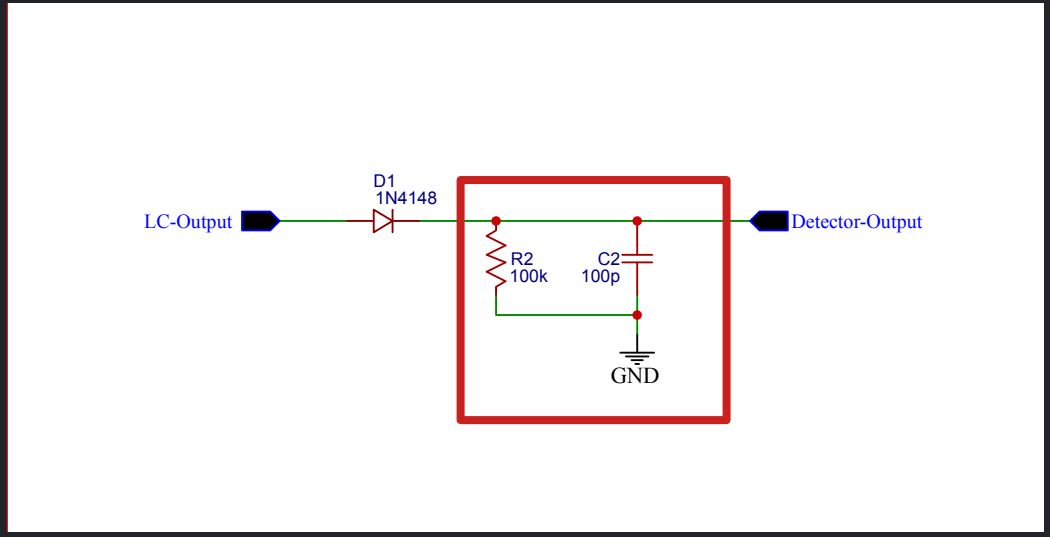
- Envelope detector

Demodulation



- Envelope detector
- Fast switching diode

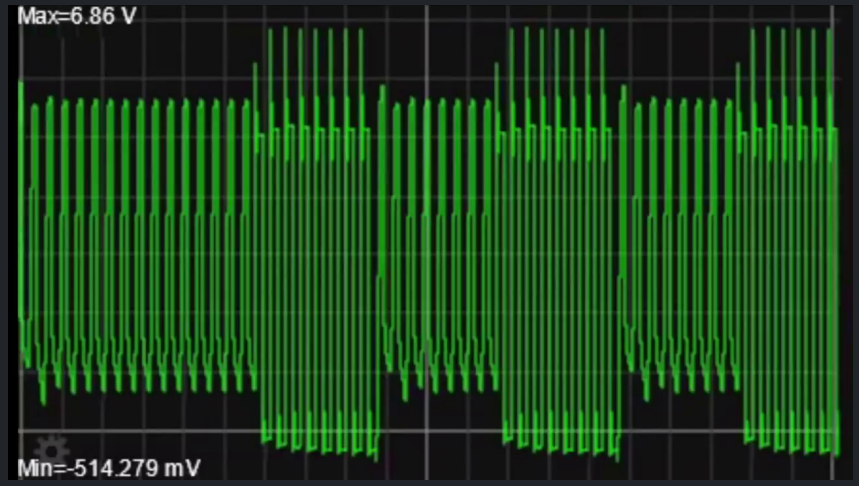
Demodulation



- Envelope detector
- Fast switching diode
- RC filter
  - $\frac{1}{134.4\,kHz} < \tau < \frac{1}{8.4\,kHz}$
  - $\tau = 0.1 \times \frac{1}{8.4\,kHz} = 11.9\,\mu s$
  - $\tau = R \times C$
  - $11.9\,\mu s \approx 100\,k\,\Omega \times 100\,pF$

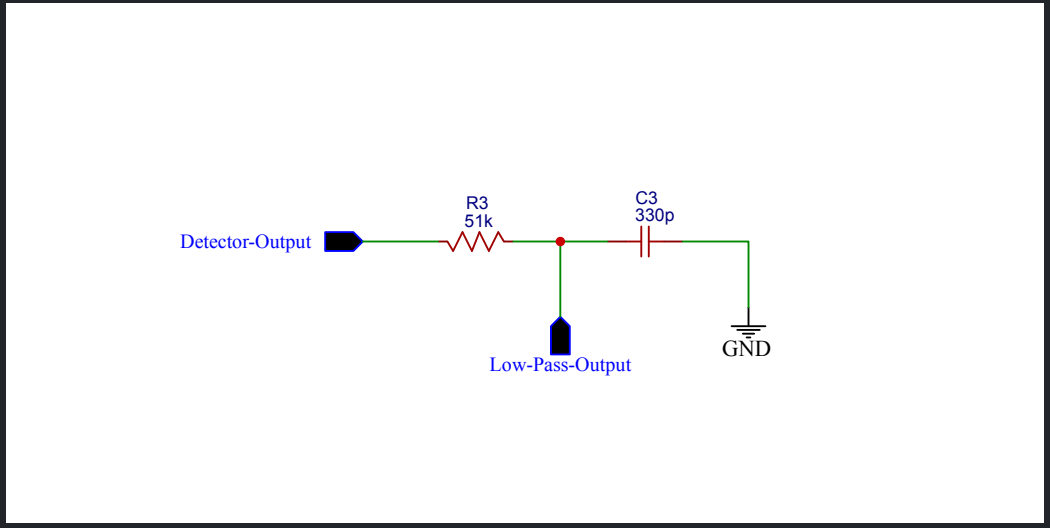
Demodulation

Reader antenna with tag (input)



Envelope detector (output)

Filtering



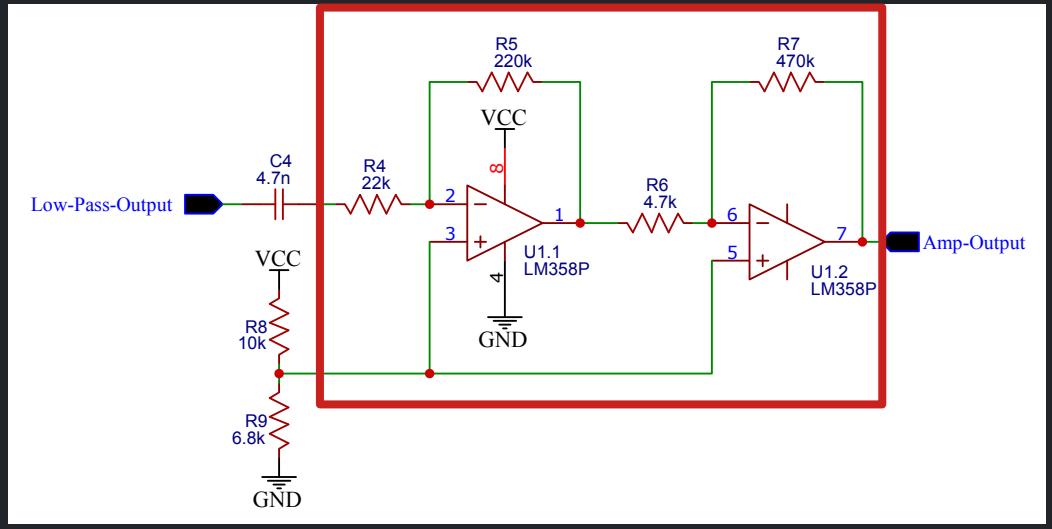
- Low-pass filter
  - $f = \frac{1}{2\pi \times R \times C}$
  - $8.4\,kHz \approx \frac{1}{2\pi \times 51\,k\,\Omega \times 330\,pF}$

Filtering

Envelope detector (input)

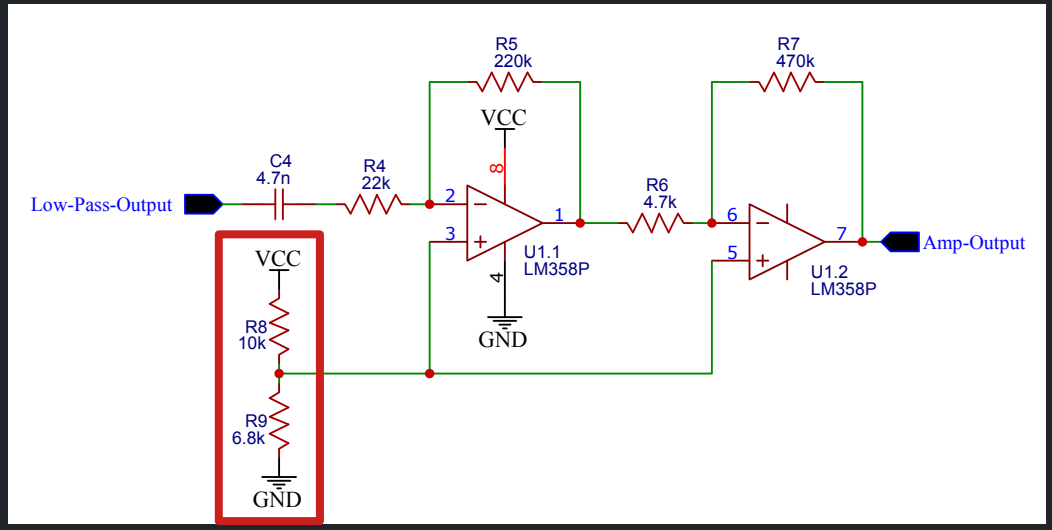
Low-pass filter (output)

Amplification



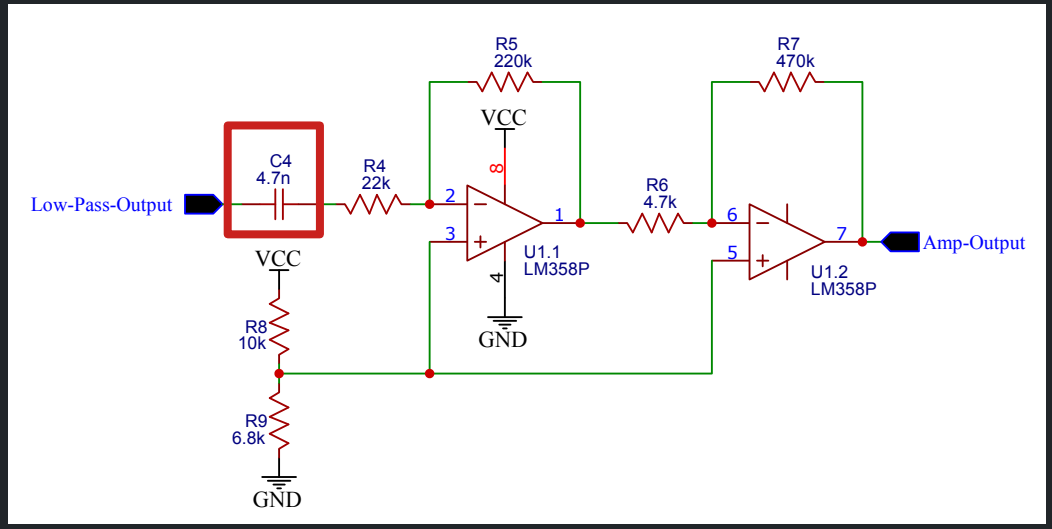
- Operational Amplifiers (op-amps)
  - Inverting configuration

Amplification



- Operational Amplifiers (op-amps)
  - Inverting configuration
- Voltage divider
  - Op-amp set point

Amplification



- Operational Amplifiers (op-amps)
  - Inverting configuration
- Voltage divider
  - Op-amp set point
- Series capacitor
  - Oscillate around set point

Amplification

Low-pass filter (input)

Op-amps (output)

Decoding

- Record time between pin changes
- Divide by half bit period
  - $119.04\,\mu s = \frac{1}{8.4\,kHz}$
- 1, 1 → 0
- 2 → 1

10	140	49	120	119	239	240	118	119	238	120	118	119	119	238	239

$$y = \frac{x}{119.04\,\mu s}$$

0	1	0	1	1	2	2	1	1	2	1	1	1	1	2	2

Bad data

0	1	1	0	1	0	0	1	1

Parsing

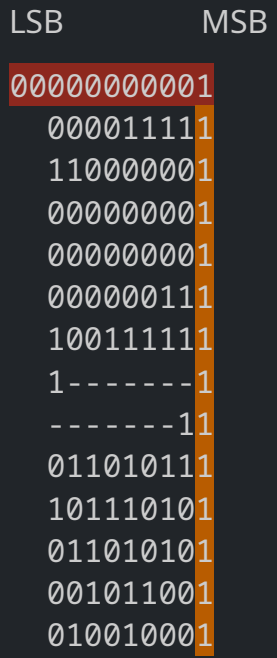
- 11-bit header

LSB MSB

```
00000000001
  000011111
  110000001
  000000001
  000000001
  000000111
  100111111
  1-------1
  -------11
  011010111
  101110101
  011010101
  001011001
  010010001
```

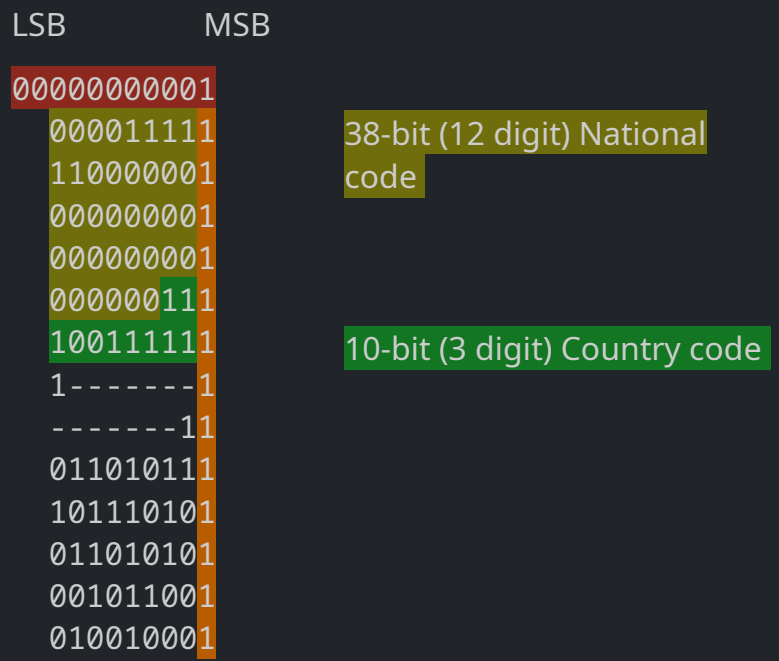
Parsing

- 11-bit header
- Control bits



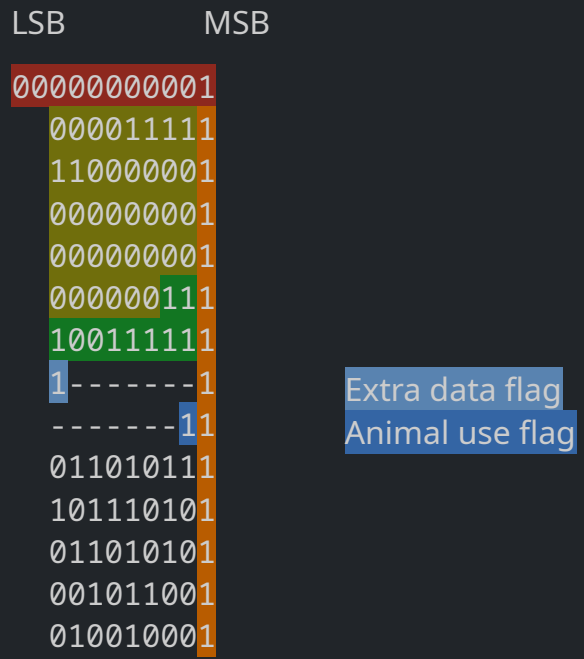
Parsing

- 11-bit header
- Control bits
- 48-bit (15 digit) unique ID



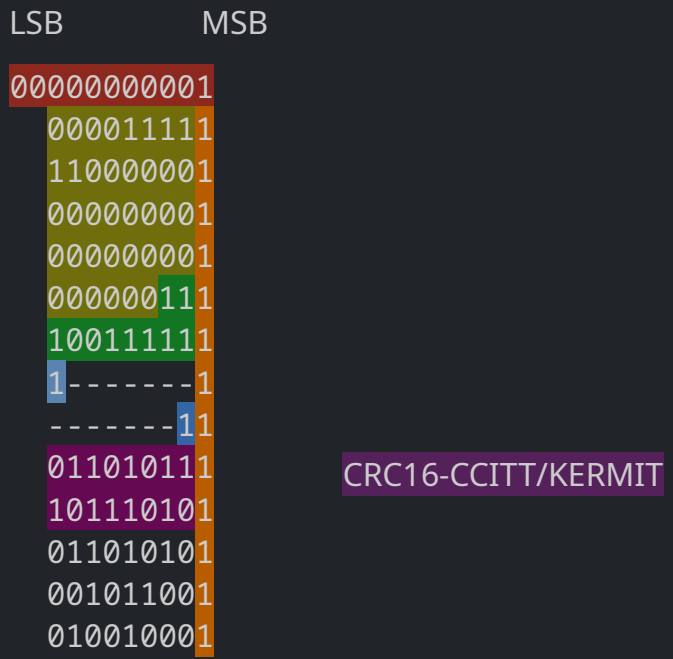
Parsing

- 11-bit header
- Control bits
- 48-bit (15 digit) unique ID
- Flags



Parsing

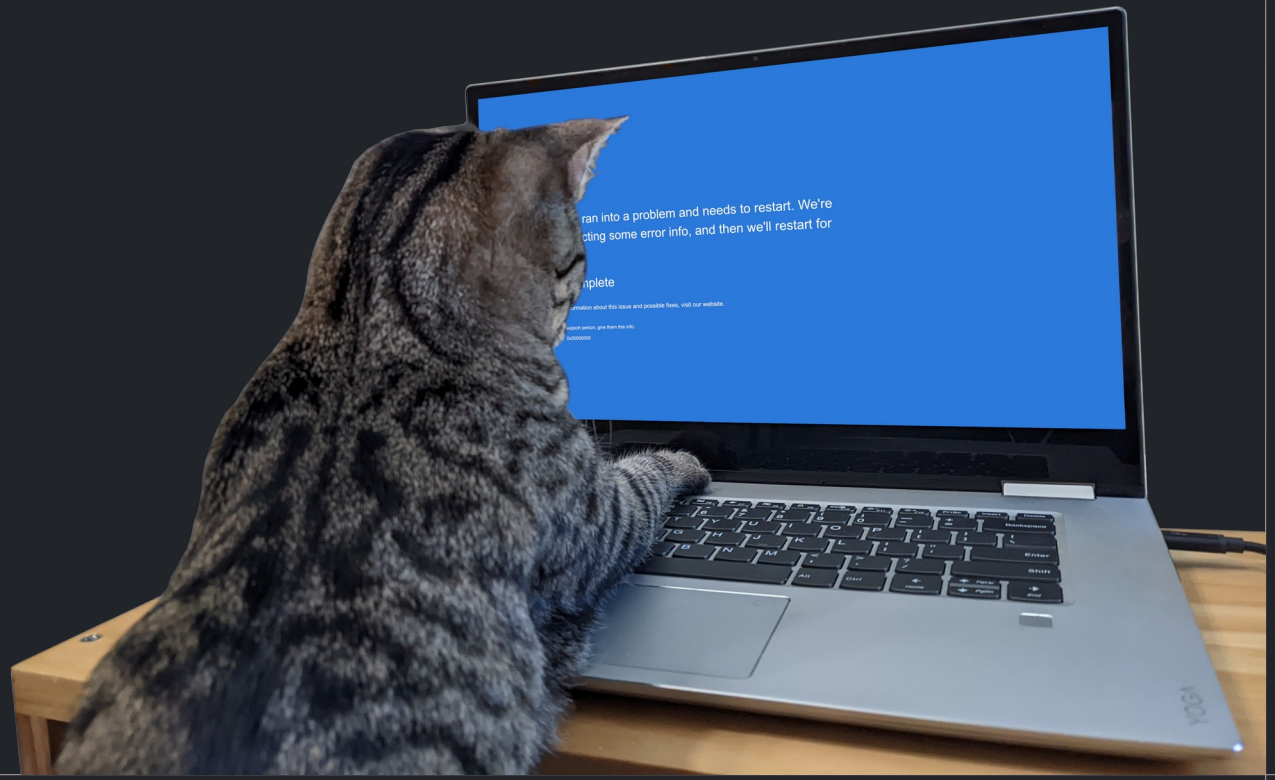
- 11-bit header
- Control bits
- 48-bit (15 digit) unique ID
- Flags
- Checksum



Parsing

- 11-bit header
- Control bits
- 48-bit (15 digit) unique ID
- Flags
- Checksum
- Extra data

Demo time


ran into a problem and needs to restart. We're
cting some error info, and then we'll restart for
nplete

Story time

- Tested on bare RFID tags
  - It works!
- Tested on cats
  - It works?

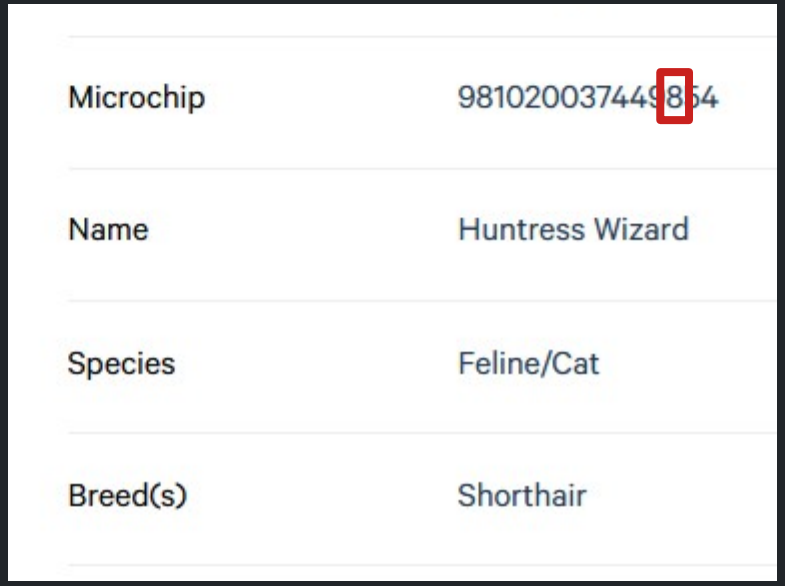
```
Ready!
Success!
981020037449754
This tag is intended for animal use
=====================================
Success!
981020037449754
This tag is intended for animal use
=====================================
Success!
981020037449754
This tag is intended for animal use
=====================================
Success!
981020037449754
This tag is intended for animal use
```

Story time

Microchip	981020037449854
Name	Huntress Wizard
Species	Feline/Cat
Breed(s)	Shorthair

```
Ready!
Success!
981020037449754
This tag is intended for animal use
=====================================
Success!
981020037449754
This tag is intended for animal use
=====================================
Success!
981020037449754
This tag is intended for animal use
=====================================
Success!
981020037449754
This tag is intended for animal use
```

Story time

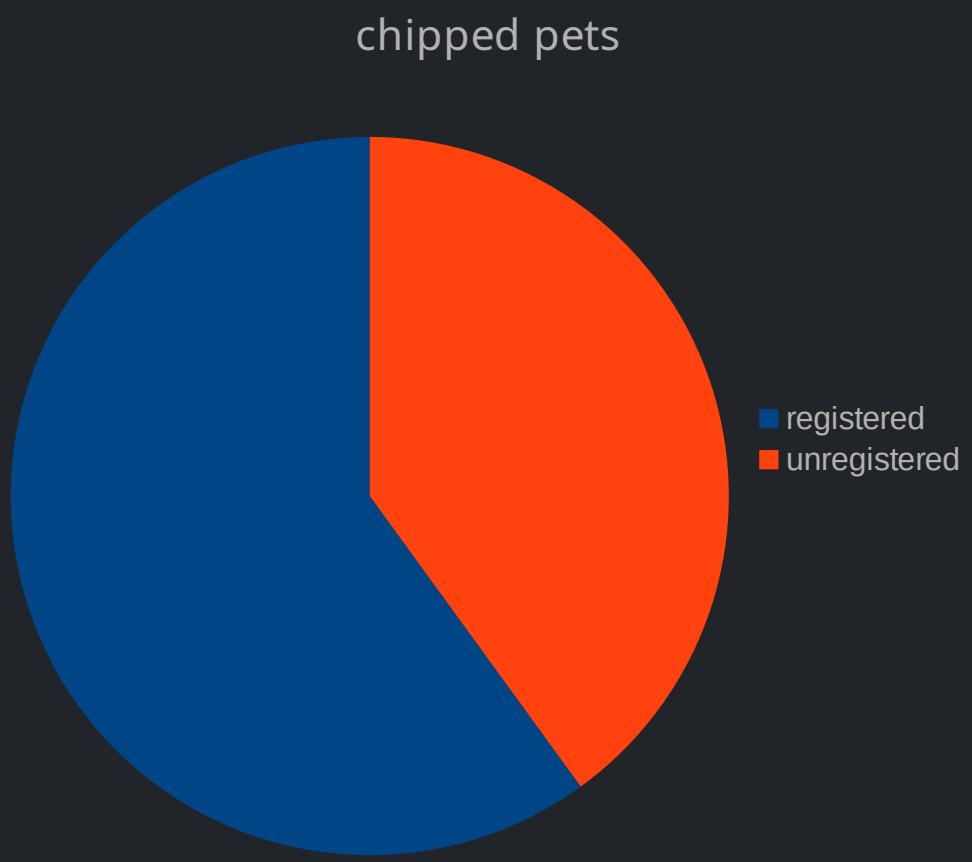


Microchip	9810200374498[illegible]64
Name	Huntress Wizard
Species	Feline/Cat
Breed(s)	Shorthair

```
Ready!
Success!
9810200374497[illegible]64
This tag is intended for animal use
=====================================
Success!
981020037449754
This tag is intended for animal use
=====================================
Success!
981020037449754
This tag is intended for animal use
=====================================
Success!
981020037449754
This tag is intended for animal use
```

Pet Microchip Registrations

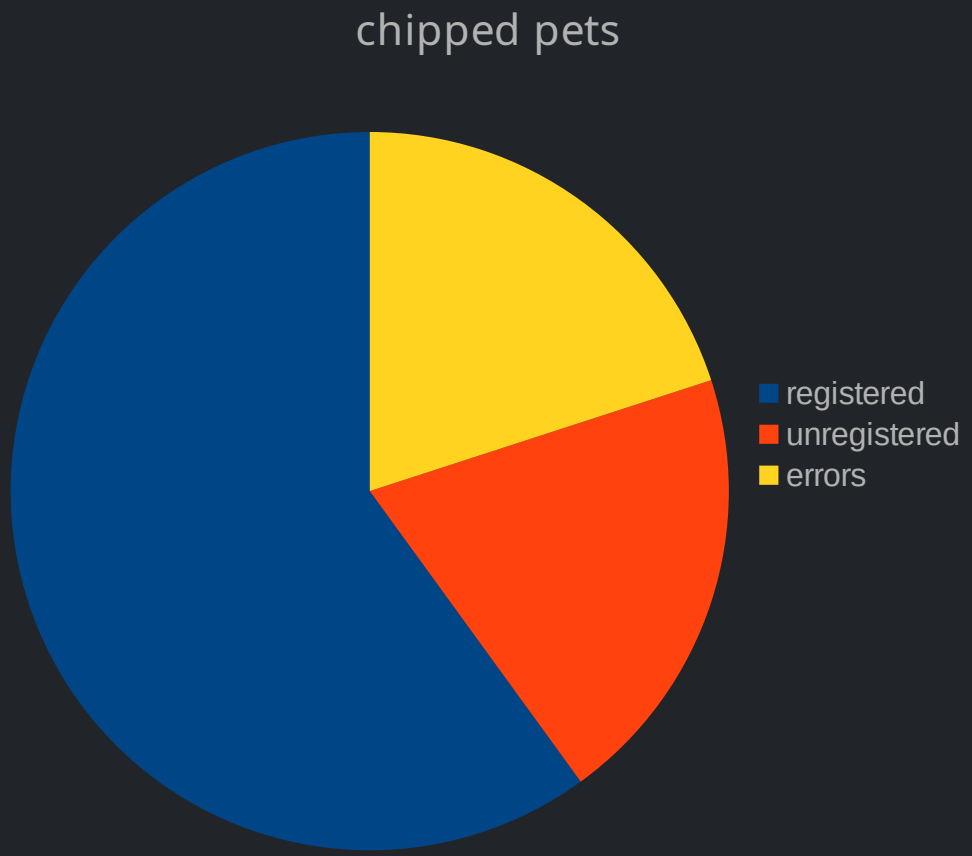
40% of microchipped pets are “unregistered”.



Pet Microchip Registrations

40% of microchipped pets are “unregistered”.

Some “unregistered” pets are the result of clerical errors.



Lessons for engineers

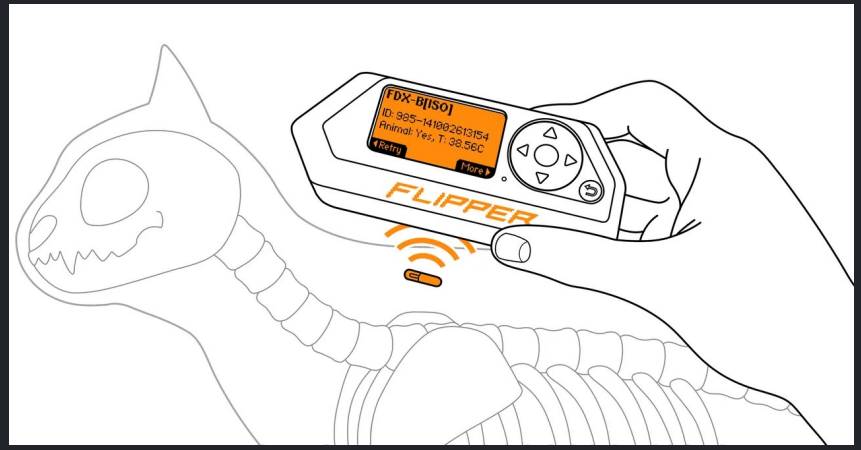
- Humans suck!!!
- Checksums rule!
- So do parity bits!

Lessons for pet owners

- Check the chip!

Lessons for pet owners

- Check the chip!
  - Flipper



Lessons for pet owners

- Check the chip!
  - Flipper
  - Ask your vet

Thank You

SecretCon 2 | Dale Cook

https://github.com/decrazyo/fdxb

https://www.youtube.com/@decrazyo