MEGACODE® to facility gates

31C3

Hamburg

2014-12-29

Kevin Redon

31st Chaos Communication Congress

EICE

a new dawn

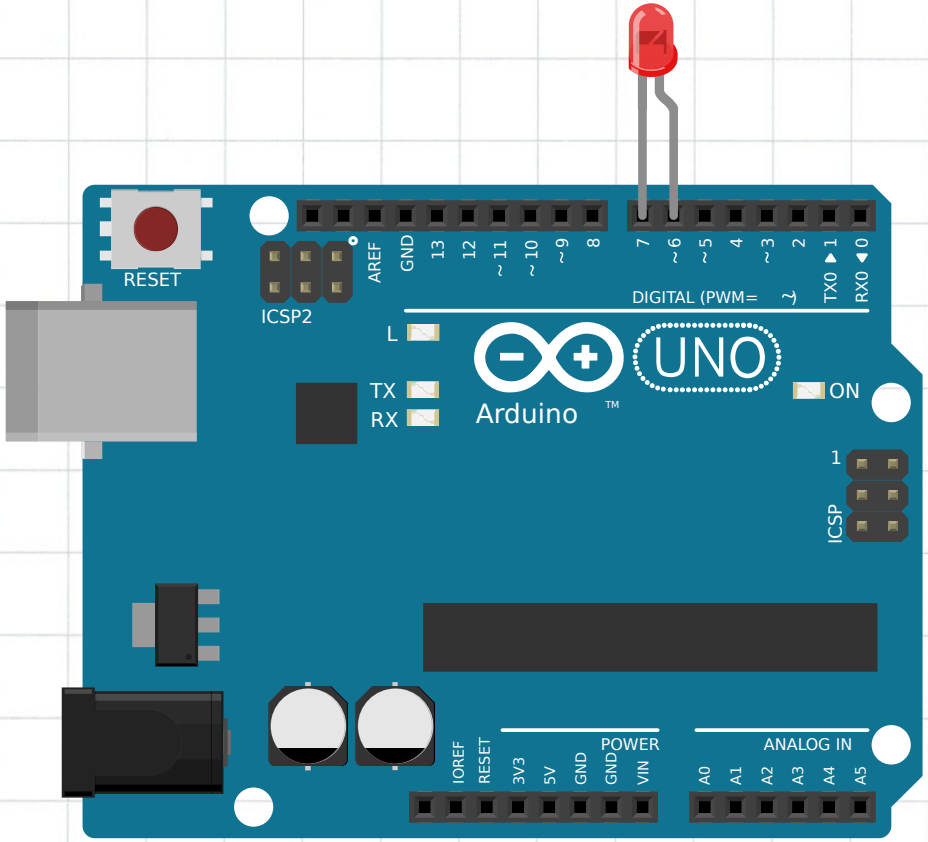
presentation

what this talk will be about:

- about PCBs, micro-controllers, and SDR
  - at a beginner level
- less technical and detailed
  - more material is linked
- not a new attack or break through
  - a simple individual fixed code replay

presentation

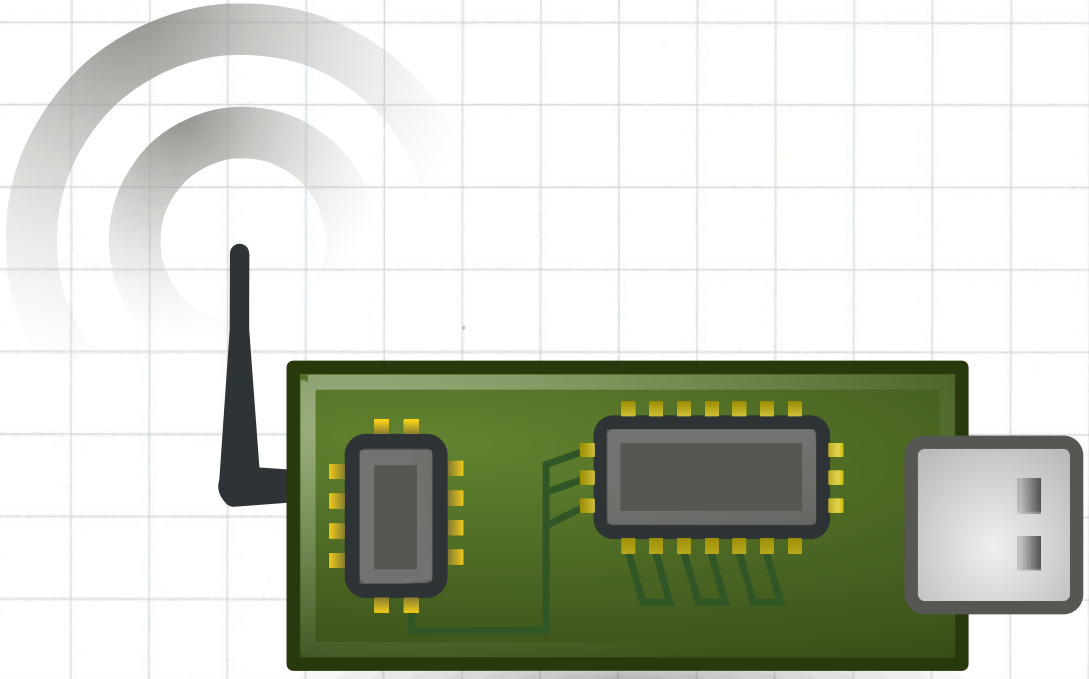
you want to do electronics



but don't know what

presentation

you want to do software defined radio (SDR)



but radio transmission is too complicated

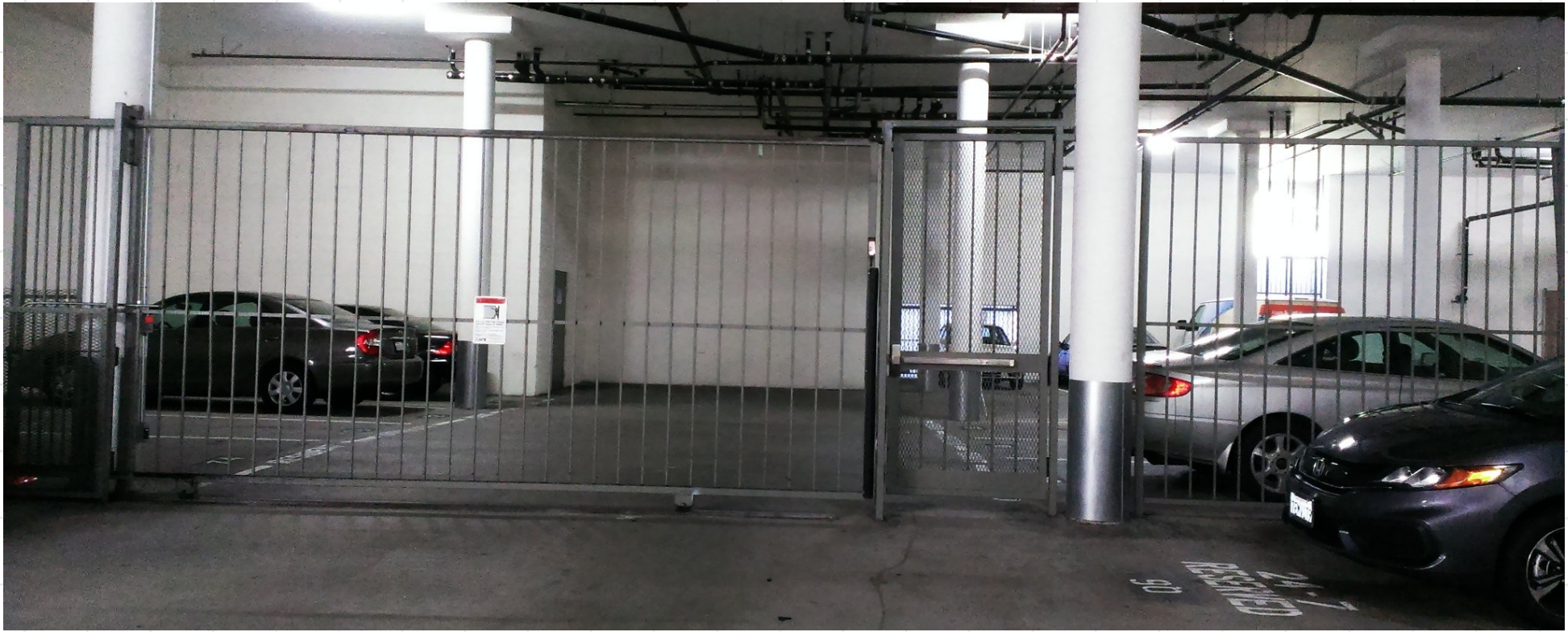
Ø – the remote

my remote to access the facility

how secure is the access to my building?

Ø - the remote

mainly used to access the garage



Ø - the remote

but also for the main entrance

usually I provide the picture's source, but this is an official picture, and I'm not sure if it's responsible to reveal the in-secure location.

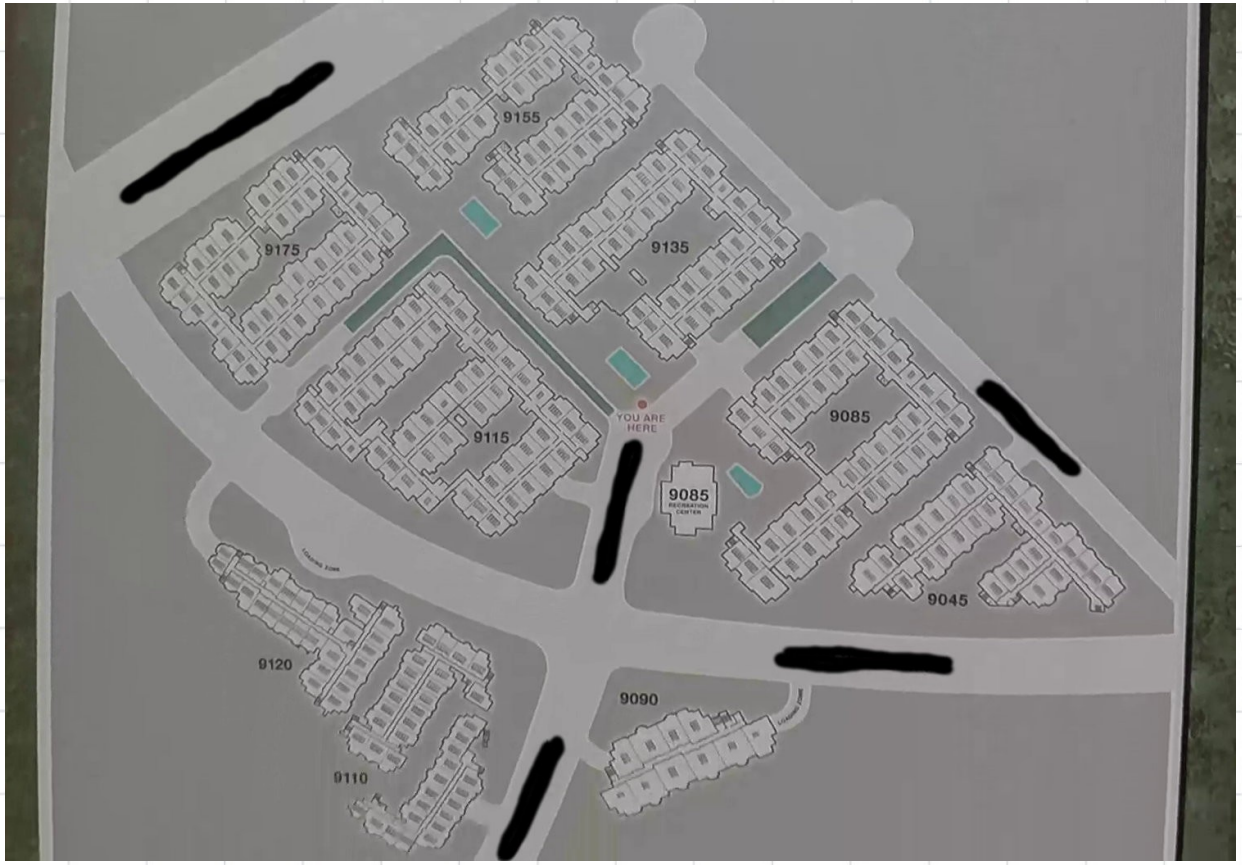
Ø - the remote

even the pool area

the hot tub will play an important role

Ø - the remote

there are a number of buildings



and normally you only have access to yours

1 - gathering information

hacking is not only about code

researching in the beginning will save you time later on

1 - gathering information

let's find out more about the remote

not a lot of information on the front

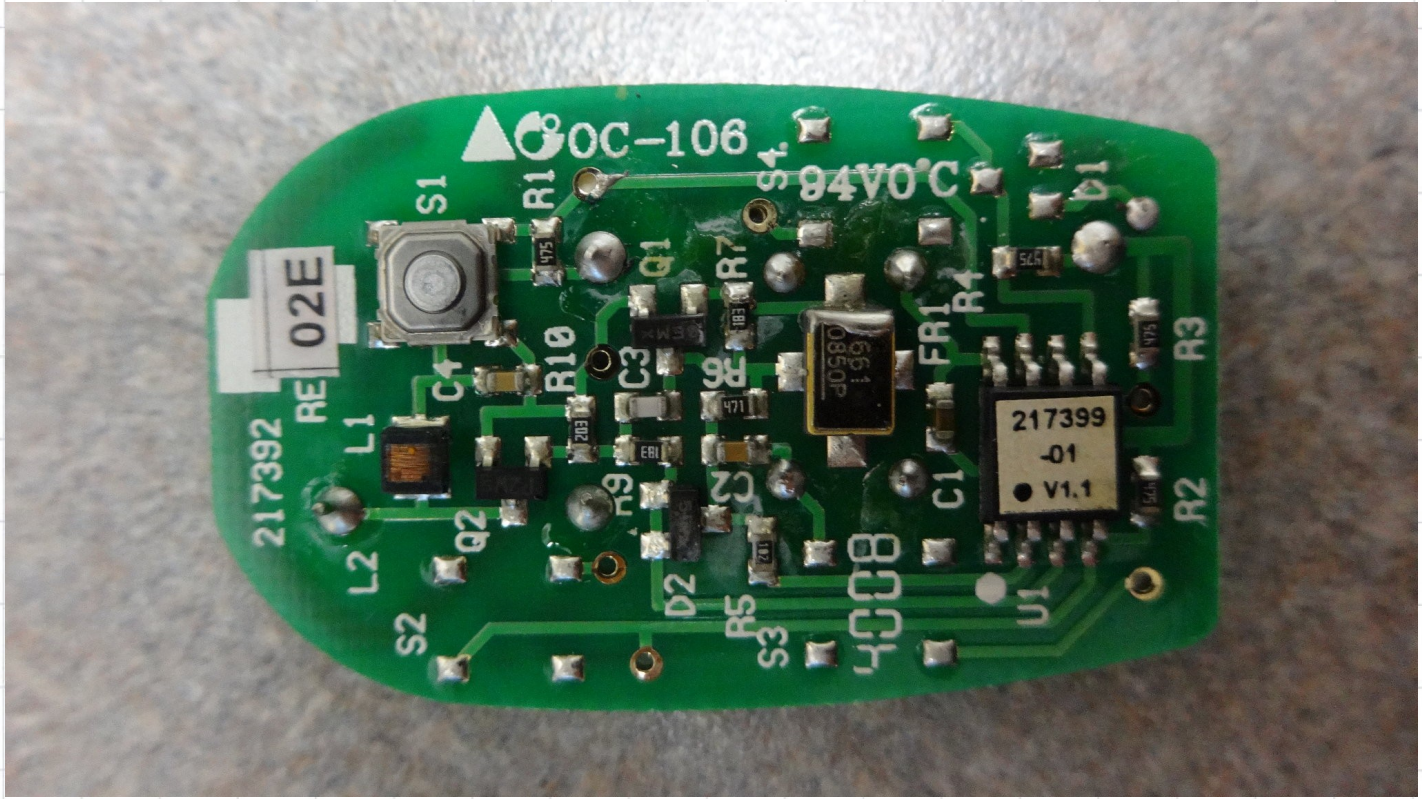
1 - gathering information

no description on the back

isn't there a sticker missing?

1 - gathering information

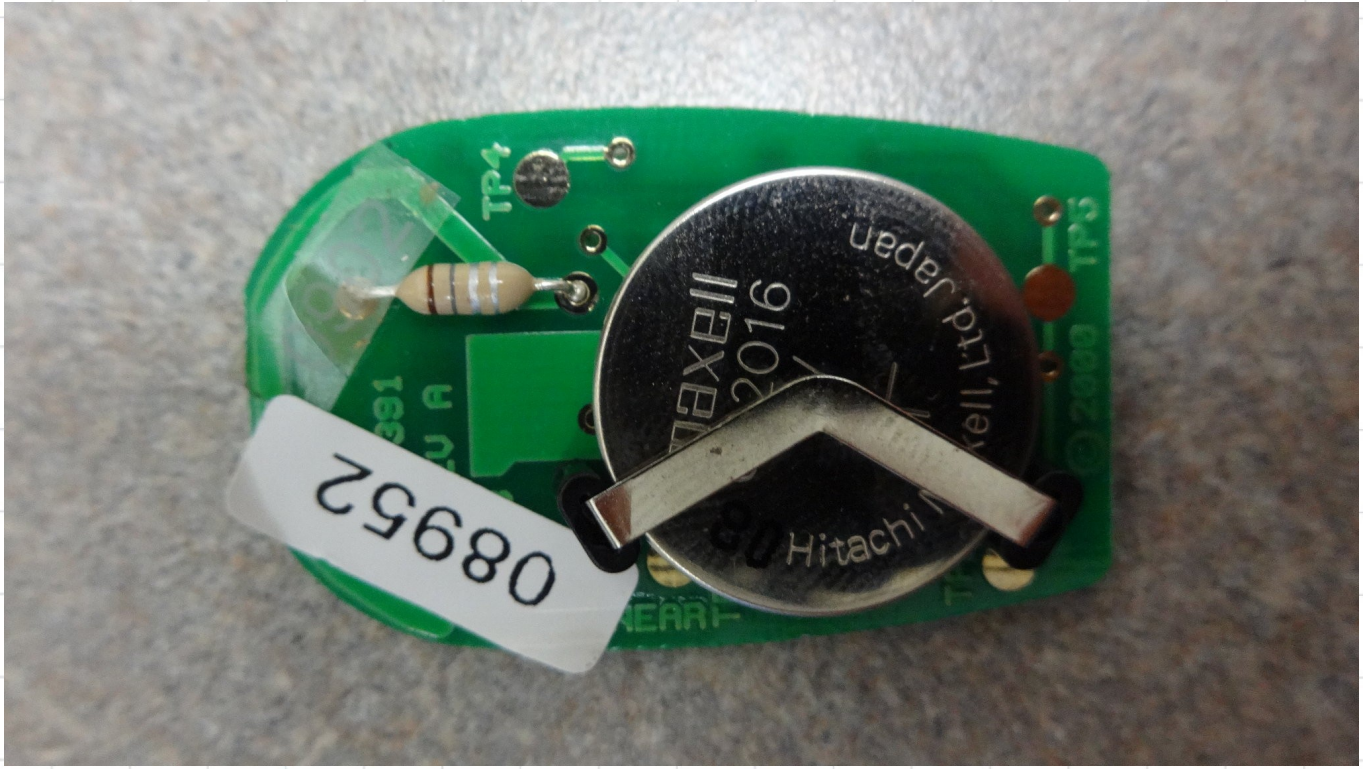
let's have a look inside



no product name or vendor

1 - gathering information

no luck with the remote



some codes but I still did not figure out what they mean

1 - gathering information

let's have a look at the receiver

the motor is just triggered by the receiver

but there is no marking on the receiver

1 - gathering information

same at the pool gate

no marking on the receiver

1 - gathering information

finally some information at the main entry

now we know at least the manufacturer: Linear

1 - gathering information

after all your efforts, time to relax

and use your social skills

1 - gathering information

ask to have a look at his remote

here is the sticker

it's a Linear ACT-34B

1 - gathering information

now we identified the vendor and product

Linear® Building On Innovation. 50

Search

Home | Products | OEM Solutions | Sales | Support | Company

ACT-34B: 4-Channel Block Coded Key Ring Transmitter

+LARGER IMAGE

The Model ACT-34B 4-Channel Block Coded Key Ring Transmitter is designed for use with Linear's access control products. The Model ACT-34B is a four-channel device supplied with a quick-disconnect key ring. Also included are lithium batteries with a five-year service life. A unique 10-second time-out feature prevents the system from being shut down by a single transmitter transmitting continuously.

The transmitter is MegaCode format, which means each transmitter is factory preprogrammed with one of over 1,000,000 codes, virtually eliminating the possibility of code duplication. Because the receiver "learns" each specific code, no unauthorized person can gain access to the system by reprogramming a transmitter.

Block coded transmitters are factory programmed to a sequential series of transmitter ID codes. When used with a Linear access controller, transmitters can be locally or remotely programmed into memory by entering the first and last codes of the block into the system. Facility codes can be selected to further customize the system.

Features

- Compatible with all Linear access receivers and controllers
- Supplied with quick-disconnect key ring
- Sold in lots of 10
- Power: Two 2016

...Read More

Specifications | Documentation | Accessories & Compatible Models

ACT-34B	
Frequency:	318 MHz
Number of Codes:	1,000,000 plus
Code Set Method:	Factory programmed
Channels:	four-channel
Power:	two 3V 2016 style batteries
Dimensions:	1.25" W x 2.25" H x .48" D (32 x 57 x 12 mm)

from the MegaCdoe series

it transmits at 318 MHz

and can have 1 000 000 codes

1 - gathering information

have a closer look a the remote

it transmits at 318 MHz

and the FCC ID is EF4 ACP00872

1 - gathering information

Federal Communications Commission is your friend

OET Exhibits List

20 Matches found for FCC ID EF4ACP00872

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
Statement of Attestation	Attestation Statements	08/09/2000	pdf	09/06/2000
Report of Measurements 1	Attestation Statements	08/09/2000	pdf	09/06/2000
Report of Measurements 2	Attestation Statements	08/09/2000	pdf	09/06/2000
Block Diagram	Block Diagram	08/09/2000	pdf	09/06/2000
FCC ID Label	ID Label/Location Info	08/09/2000	pdf	09/06/2000
id label	ID Label/Location Info	08/29/2000	pdf	09/06/2000
Internal External Photos 2 Pages	Internal Photos	08/09/2000	pdf	09/06/2000
Functional Description	Operational Description	08/09/2000	pdf	09/06/2000
Parts List	Parts List/Tune Up Info	08/09/2000	pdf	09/06/2000
Schematics 2	Schematics	08/09/2000	pdf	09/06/2000
Schematics 1	Schematics	08/09/2000	pdf	09/06/2000
Report	Test Report	08/09/2000	pdf	09/06/2000
Test Report	Test Report	08/09/2000	pdf	09/06/2000
Testing Instrumentation List	Test Report	08/09/2000	pdf	09/06/2000
Measurement of Radio Freq Emission	Test Report	08/09/2000	pdf	09/06/2000
Duration of RF Transmissions	Test Report	08/09/2000	pdf	09/06/2000
Megacode 1	Test Report	08/09/2000	pdf	09/06/2000
Megacode 2	Test Report	08/09/2000	pdf	09/06/2000
Test Setup Photos	Test Setup Photos	08/09/2000	pdf	09/06/2000
Users Manual	Users Manual	08/09/2000	pdf	09/06/2000

it provides numerous technical documents

1 - gathering information

the test report identifies the transmission

5.0 General Technical Requirements:

5.1 Testing Methods:	Peak Signal pulse position modulated A1D signal.
5.1 Reference Standard:	C63.4-1992 (FCC Procedure)
5.2 Modulation:	Pulse Position A1D, AM Modulation
5.3 Type of Antenna:	Integral to Transmitter Case - Tuned Loop
5.4 External Controls:	Push Buttons No user serviceable parts except for replacement of batteries.

no complicated radio communication

it's a simple on/off signal

1 - gathering information

even the MegaCode transmission is described

TRANSMITTER DUTY CYCLE CALCULATIONS
AND TIME DOMAIN INFORMATION

Duty Cycle is fixed because binary-coded, pulse-position type A1A modulation is used. Modulation rate is fixed at 167 bits per second. Therefore, each bit frame occupies 6 ms.

During transmission, the transmitter sequentially emits a group of 25 pulses in the form of a pulse-keyed carrier. Each pulse (transmitter ON time) has a duration of one millisecond (ms).

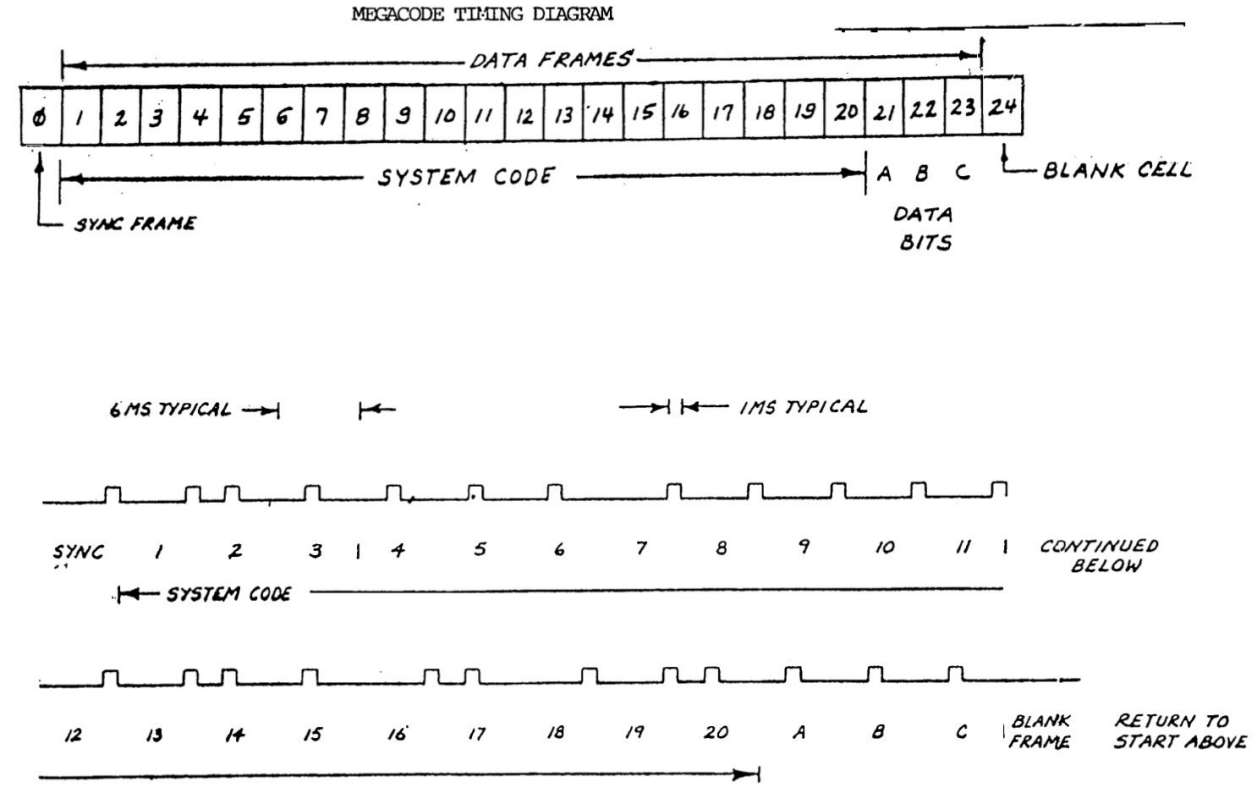
REAL TIME ANALYSIS: Refer to Page 6 for timing diagram. From time zero, one synchronization pulse of 1 ms duration occurs within a 6 ms "bitframe." Elapsed time: 6 ms.

Each of the remaining 24 information pulses occupy a 1 ms duration position within a 6 ms wide "bit frame" (24 frames) Total elapsed time: 144 ms.

24 bit frames, 6 ms frames, 1 ms pulse per frame

1 - gathering information

and there is a nice timing diagram



1 sync frame, 20 system code frames

3 data bits frames, 1 blank cell

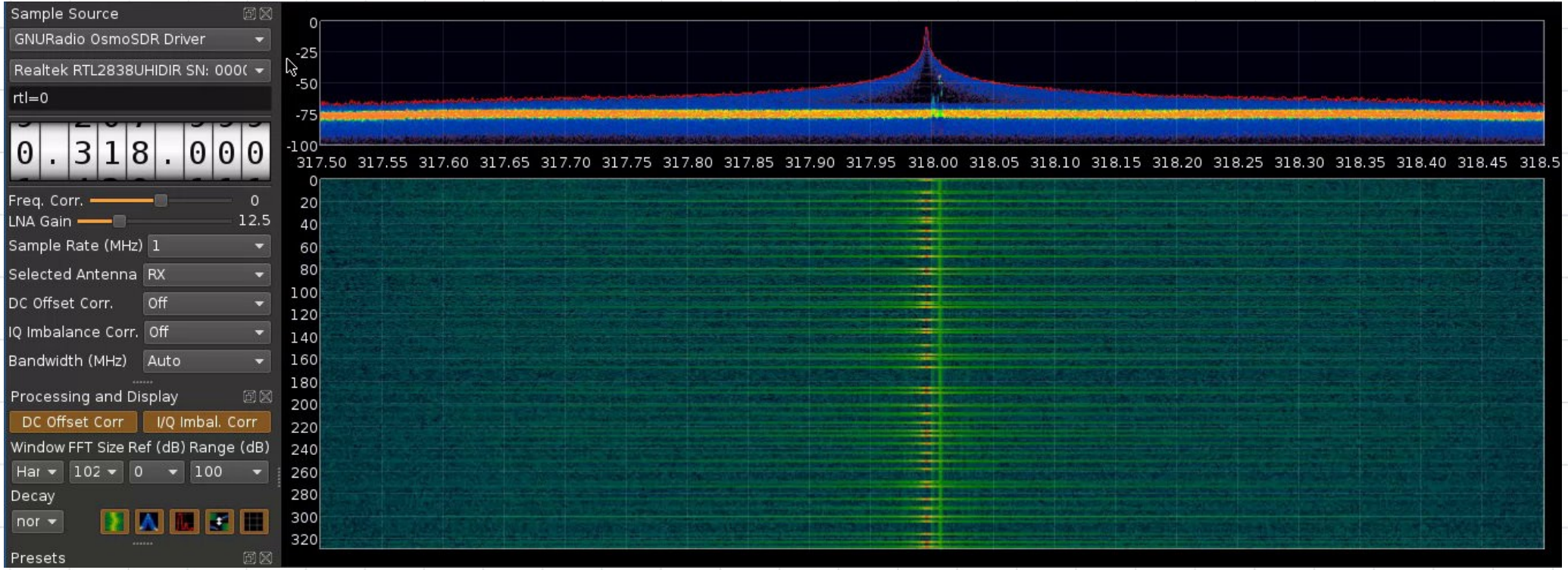
2 - MegaCode decoding

time to record the radio transmission

get a cheap RTL-SDR

2 - MegaCode decoding

tune to 318 MHz

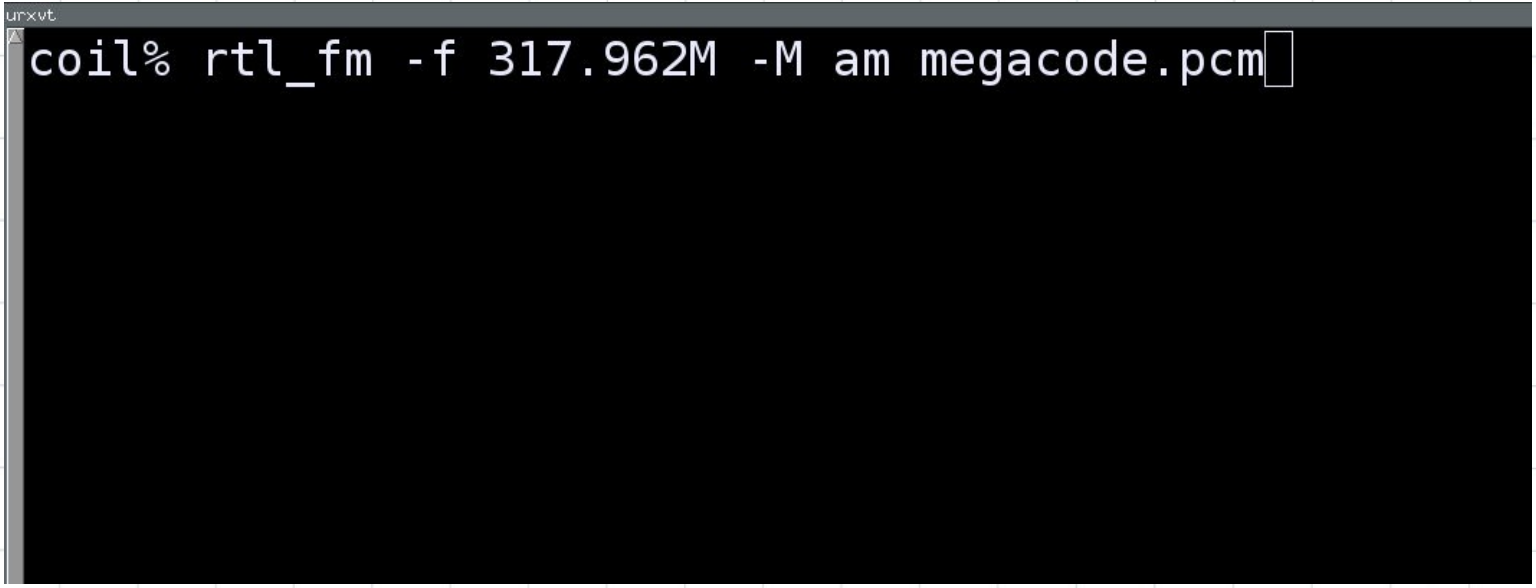


clear on/off transmission

(waterfall graph from sdrangelove)

2 - MegaCode decoding

demodulate the AM signal

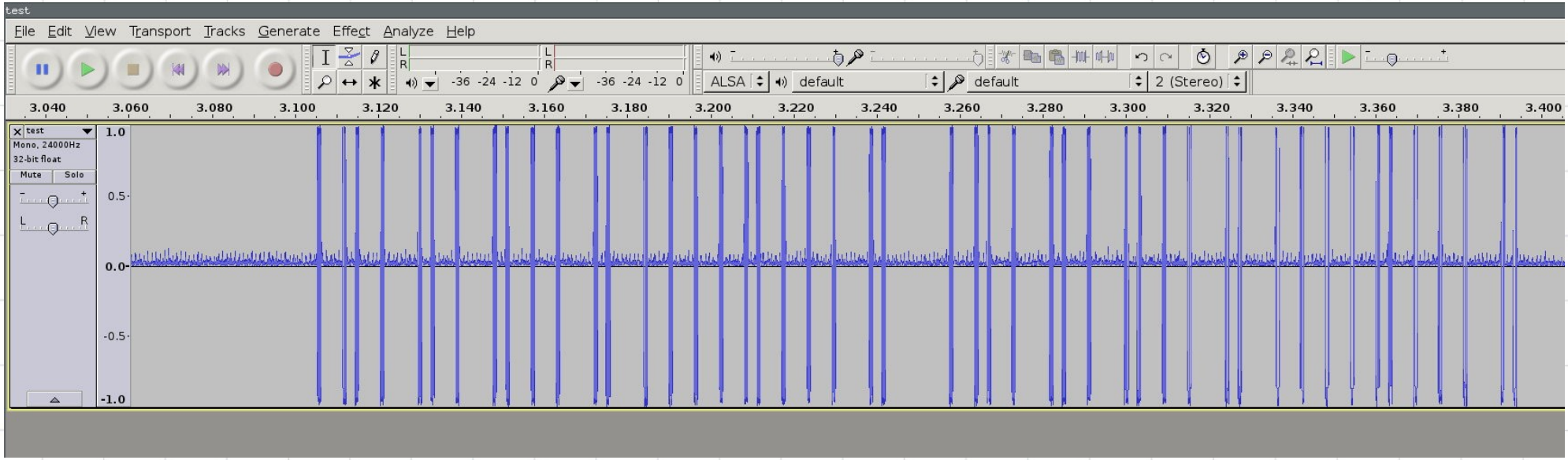


no need for GNU Radio and a complex graph

simply use rtl_fm, a radio demodulator

2 – MegaCode decoding

let's have a look at the signal



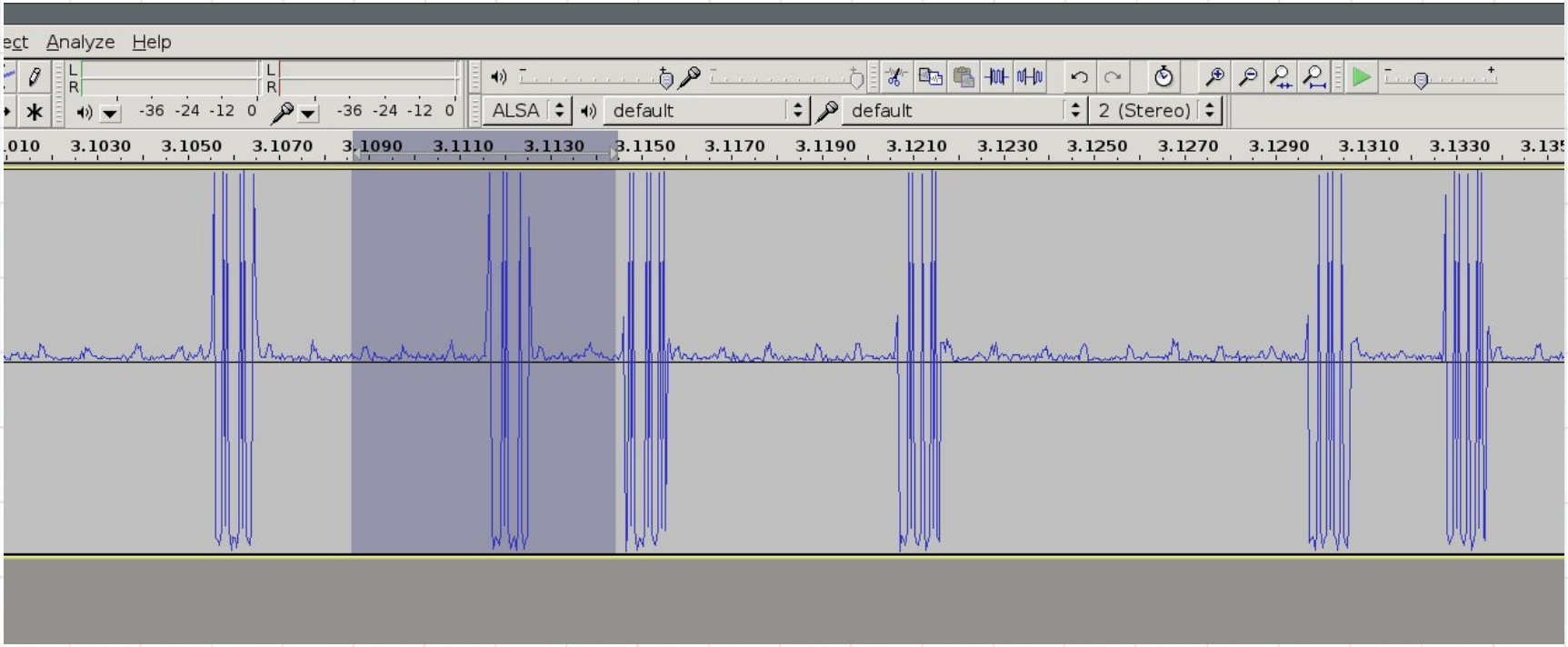
use audacity on the demodulated signal

2x24 pulses, each 1 ms long

the 2 patterns look similar

2 - MegaCode decoding

how is the data encoded?



pulse position encoding

1 ms pulse every 6 ms

pulse either in the first or second half: 0 or 1

2 - MegaCode decoding

write a decoder for the demodulated data

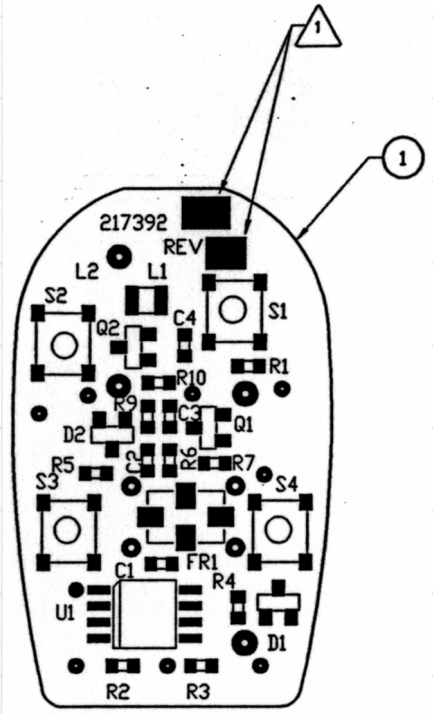
```
urxvt
coil% ./decode.rb test.pcm
# egdes: 1822
# pulses: 167
# groups: 9 (24, 24, 23, 13, 10, 24, 24, 24, 1)
# transmissions: 5
# values: 5
values:
- value: 13178818 (0xc917c2), system code: 598776 (0x922f8), databits: 2 (0x2)
- value: 13178818 (0xc917c2), system code: 598776 (0x922f8), databits: 2 (0x2)
- value: 13178818 (0xc917c2), system code: 598776 (0x922f8), databits: 2 (0x2)
- value: 13178818 (0xc917c2), system code: 598776 (0x922f8), databits: 2 (0x2)
- value: 13178818 (0xc917c2), system code: 598776 (0x922f8), databits: 2 (0x2)
coil%
```

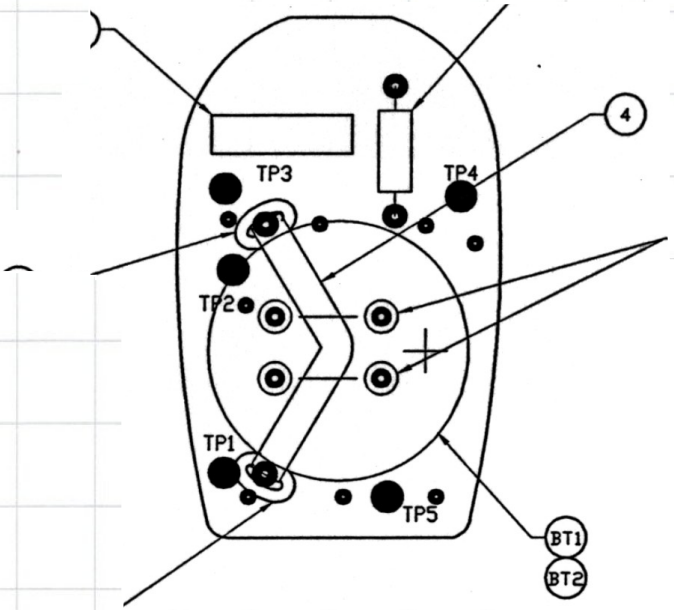
107 lines of code

exact same code repeats → fixed code → replay attack

3 - MegaCode cloning

the PCB layout is provided

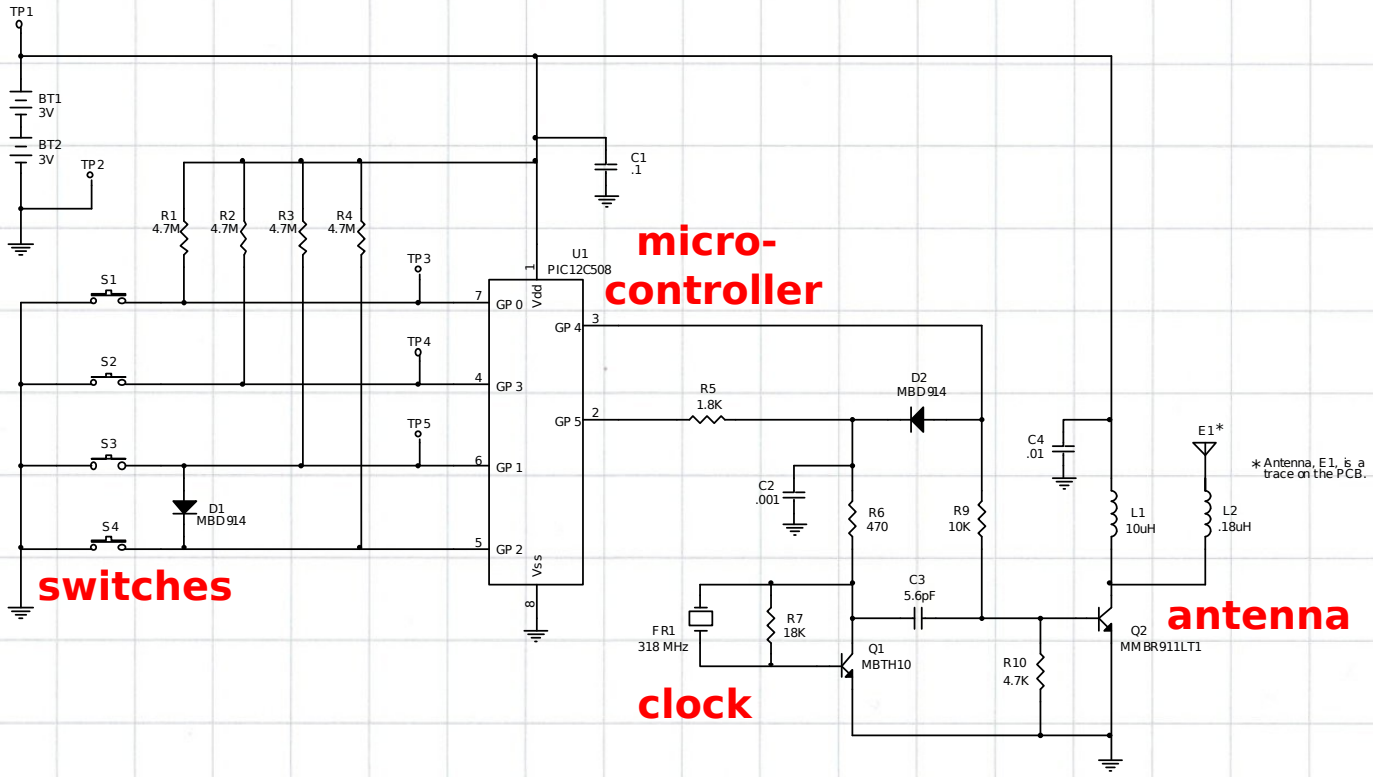




this describes where components are placed

3 – MegaCode cloning

the schematic is provided

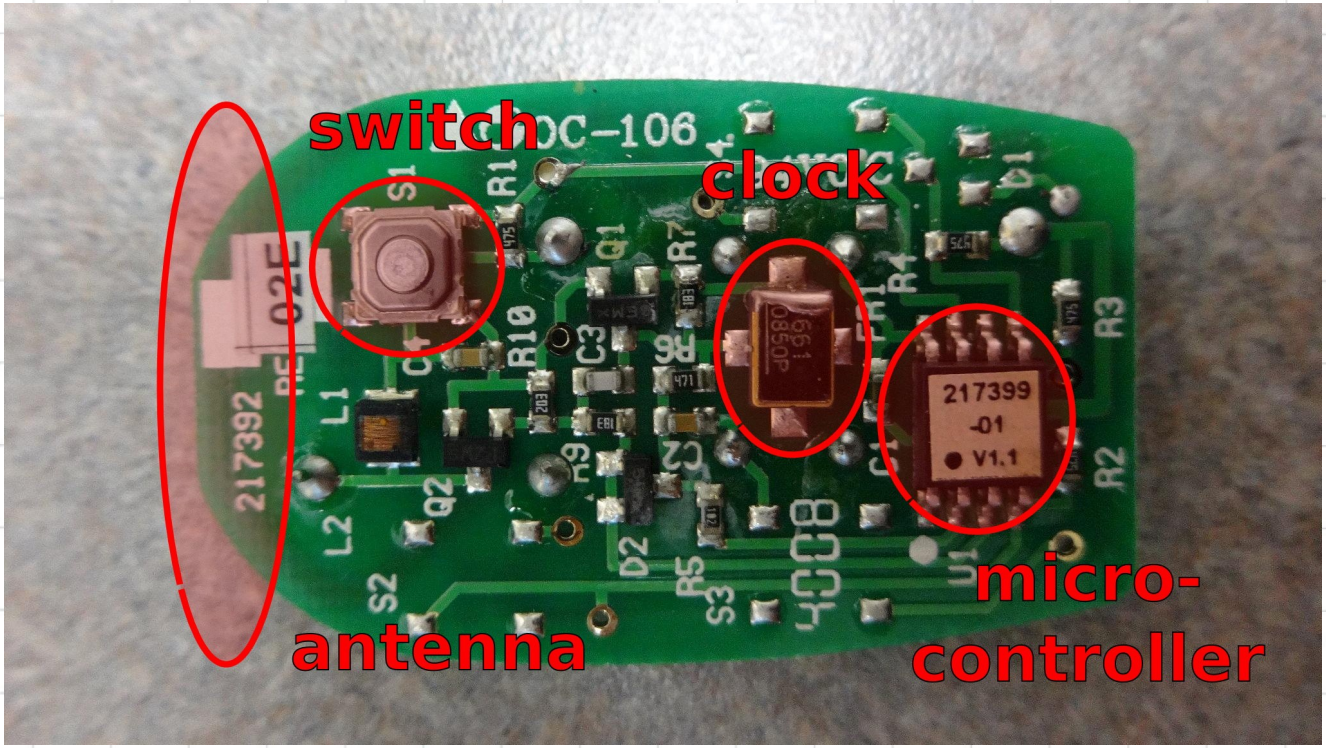


this describes which components are used

and how they are connected together

3 - MegaCode cloning

what chip is used on the remote?



simple board with few components

uses a Microchip PIC12C508A micro-controller

3 - MegaCode cloning

can we write our own code on the remote?

PIC12C508 Mature Product Buy it Now

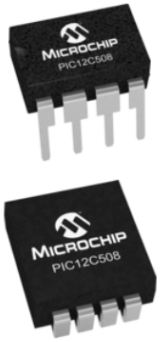
myMicrochip Login

Documentation & Software | Pricing & Samples | Development Tools | Similar Products | Quick Links

PIC12C5XX/CE5XX Datasheet (08/28/2003)

Please consider this device: PIC12F508. View Side By Side Comparison

The PIC12C5XX from Microchip Technology is a family of low-cost, high performance, 8-bit, fully static, EEPROM/EPROM/ROM-based CMOS microcontrollers. It employs a RISC architecture with only 33 single word/single cycle instructions. All instructions are single cycle (1 ms) except for program branches which take two cycles. The PIC12C5XX delivers performance an order of magnitude higher than its competitors in the same price category. The 12-bit wide instructions are highly symmetrical resulting in 2:1 code compression over other 8-bit microcontrollers in its class. The easy to use and easy to remember instruction set reduces development time significantly.
A newer device is available. Please consider PIC12F508.



Features
6 I/O pins with 25mA source/sink per I/O, 4 oscillator selections including the internal 4 MHz RC oscillator with programmable calibration, and Power-on Reset.

Parameter Name	Value
Program Memory Type	OTP
Program Memory (KB)	0.75
CPU Speed (MIPS)	1
RAM Bytes	25
Timers	1 x 8-bit
Temperature Range (C)	-40 to 125
Operating Voltage Range (V)	2.5 to 5.5
Pin Count	8

has code protection on (can't read the firmware)

one time programmable only

3 - MegaCode cloning

is there any other remote?

amazon Try Prime | Your Amazon.com | Today's Deals | Gift Cards | Sell | Help

Shop by Department | Search | All | linear megacode remote compatible | Go

17-32 of 60 results for **"linear megacode remote compatible"**

Show results for

Tools & Home Improvement ›

Electronics ›

Automotive ›

Refine by

Linear ACT-21A 318MHz MegaCode 1-Channel Key Ring Transmitter

by Linear

$15.00

Only 6 left in stock - order soon.

More Buying Choices

$10.32 new (18 offers)

★★★★½ ▾ 20

Product Features

... *Compatible* with 318MHz *Linear* access receivers ... *MegaCode* ...

Tools & Home Improvement: See all 49 items

Linear ACT31B/21B Compatible Keychain Remote

by Transmitter Solutions

$14.99

Only 8 left in stock - order soon.

More Buying Choices

$14.99 new (5 offers)

★★★★★ ▾ 3

Product Features

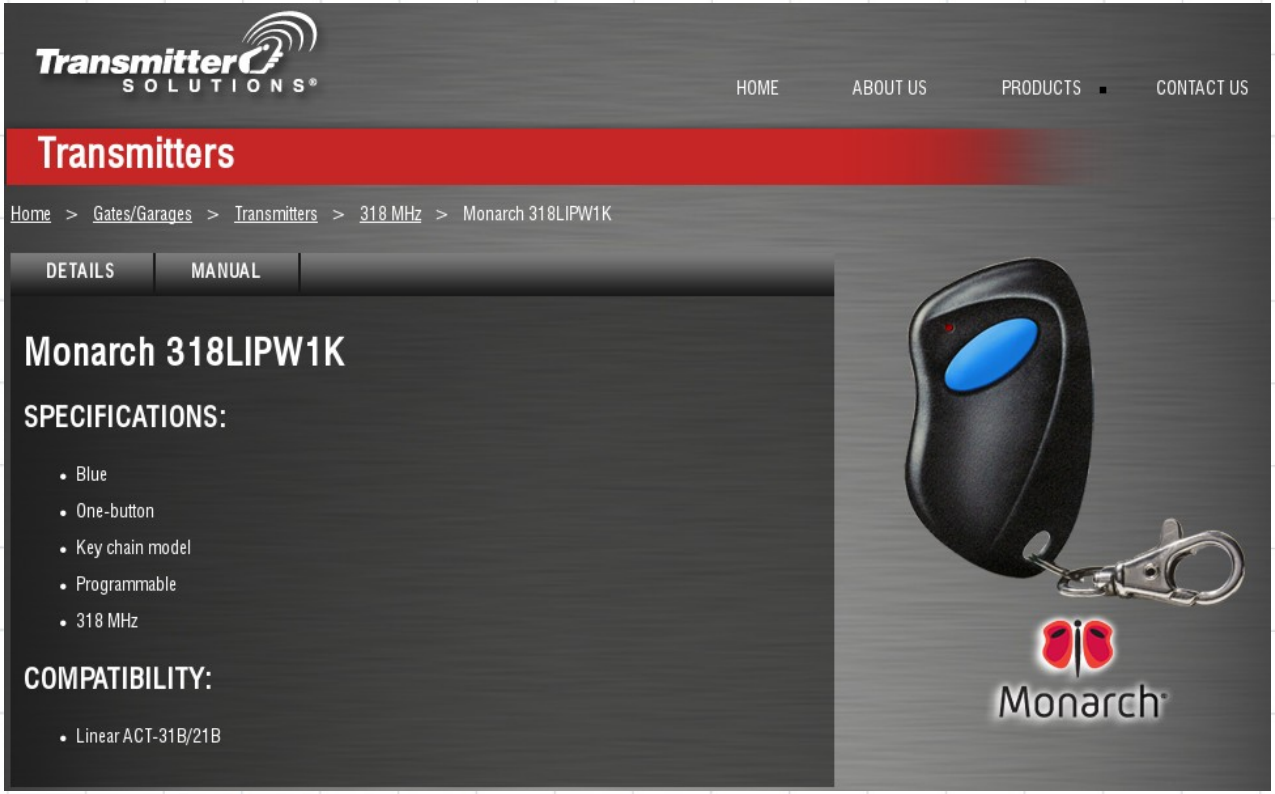
Operates with *Linear MegaCode* receivers and transmitters

Tools & Home Improvement: See all 49 items

the system is so simply, someone probably already created a compatible remote

3 - MegaCode cloning

look for vendor information



matches: 318 MHz, compatible with ACT-31B

and apparently it is even programmable

3 - MegaCode cloning

look at the manual

2 - NUMBERING

Each transmitter is manufactured and sold with a different factory-set serial number .

3 - PROGRAMMING

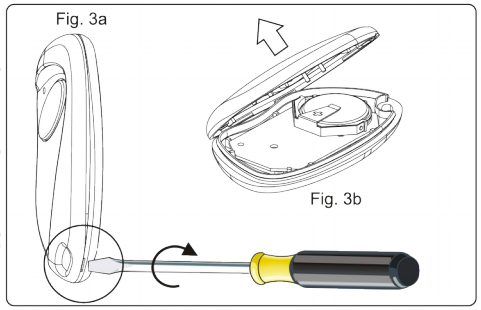
The transmitter must be programmed into your system memory.
Your own installer or reseller will provide you the necessary instructions for your system.

4 - OPERATION

A - Firmly depress the button until the small red LED illuminates.
B - After the LED has illuminated, release the button.
If the device you are attempting to activate does not respond, repeat steps A and B or consult section 6 (Troubleshooting) of this manual.

5 - BATTERY ACCESS

To access the battery open the case with a screwdriver acting on the slot between the cover and the bottom and remove the bottom, as shown in fig. 3a and 3b. Slide out the old batteries and replace them with the new ones [CR2016] respecting the polarity, with the positive (+) side upward.
NOTE: Please dispose of the batteries properly according to local laws and regulations.
Test proper battery installation by verifying that the red LED illuminates when the button is pushed.



6 - TROUBLESHOOTING

PROBLEM	SOLUTION
The system does not receiver the transmitter signal. The transmitter LED will not light	Replace the transmitter batteries
The system does not receiver the transmitter signal. The transmitter LED is ON	Check to verify the transmitter is programmed into your system
The operating range is reduced	Replace the transmitter batteries

Transmitter Solutions - Type : 318LIPW1K

FCC ID : SU7318LIPW1K

This device complies with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) this device must accept interference received, including interference that may cause undesired operation.

Notice

Any changes or modification to Transmitter Solutions equipment not expressly approved by Transmitter Solutions could void the manufacturer's warranty.

WARRANTY

The warranty period of Transmitter Solutions 318 transmitters is 60 months, beginning from the manufacturing date of the transmitter. During this period, if the product does not operate correctly, due to a defective component, the product will be repaired or replaced at the sole discretion of Transmitter Solutions. The warranty does not extend to the transmitter case which can be damaged by conditions outside the control of Transmitter Solutions or to battery life.

Monarch

TRANSMITTER SOLUTIONS
7380 S. Eastern Ave, Ste 124-320
Las Vegas, NV 89123 -
(866) 975-0101 - (866) 975-0404 F
sales@transmittersolutions.com

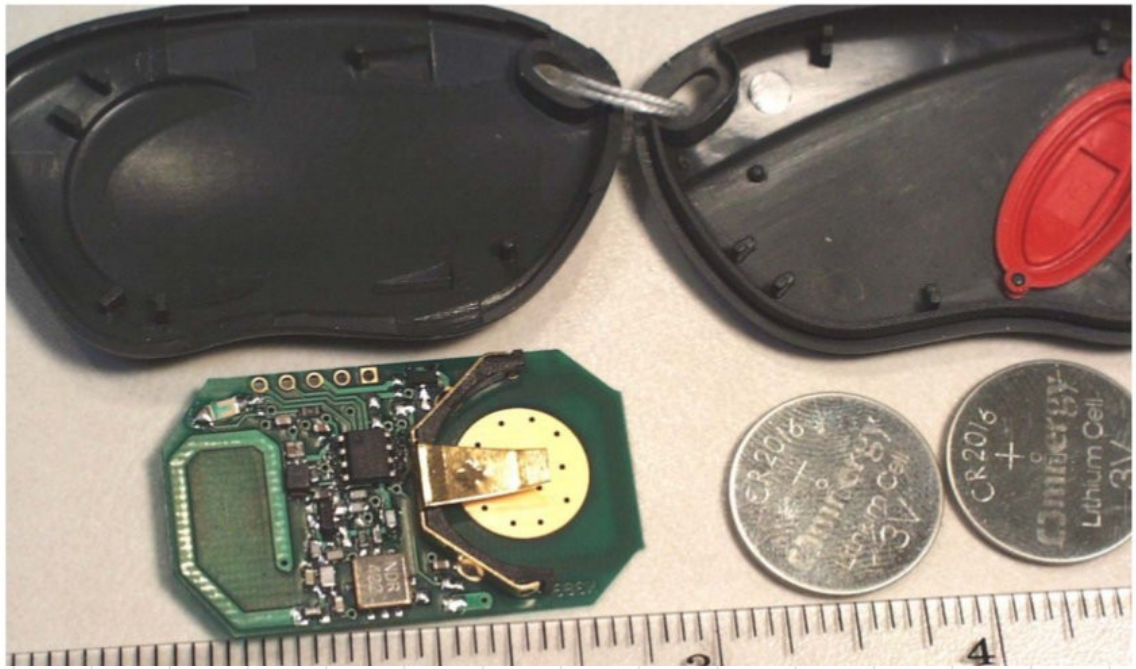
not a lot of information on how to program it

but it provides the FCC ID

3 - MegaCode cloning

look at the FCC documents

View of the Component Side of the PCB



they don't even mention the encoding

but provide an internal picture, with a pin header

3 - MegaCode cloning

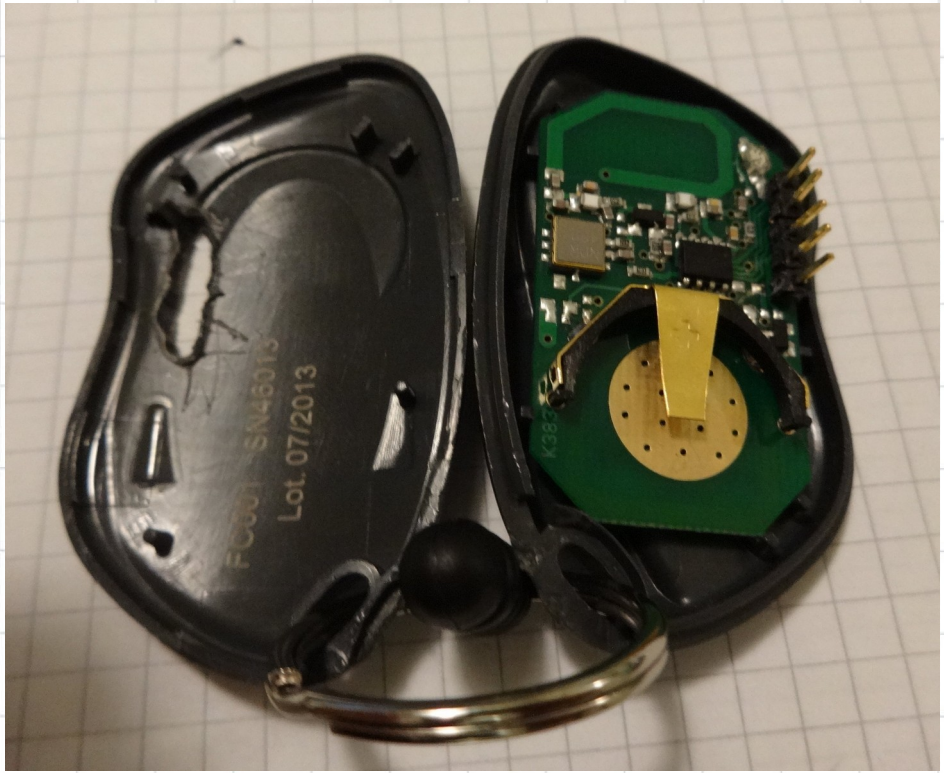
get the remote

the programming header is there

and it uses a re-programmable Microchip PIC12F629

3 - MegaCode cloning

get the remote

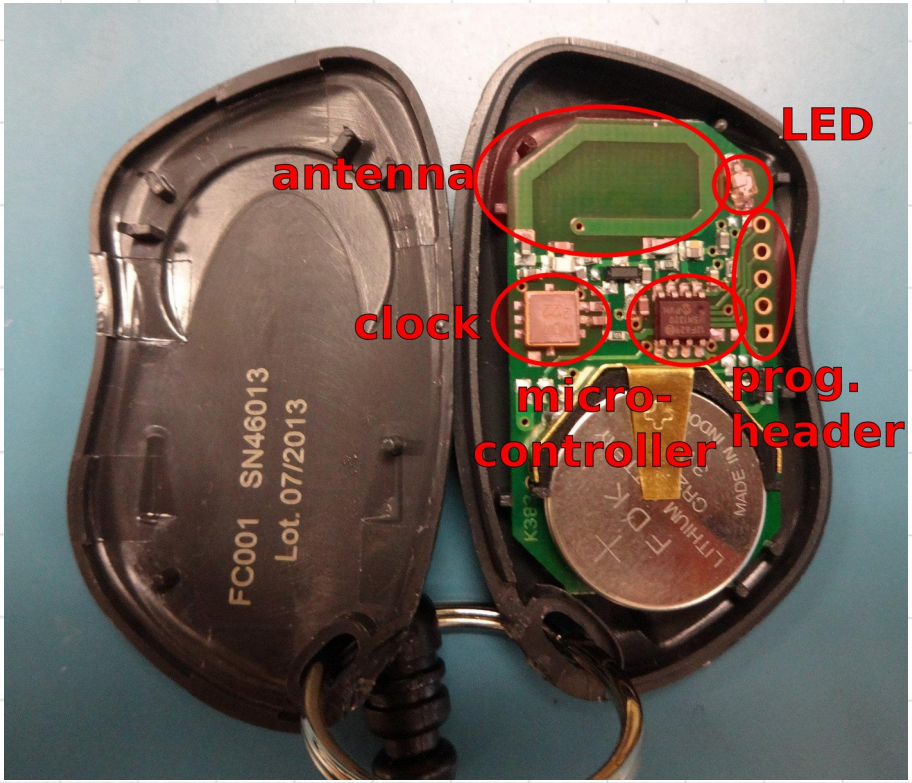


easy soldering, ideal for newcomers

chip is flash based and supported by the PICkit2 programmer

3 - MegaCode cloning

identify components and connections

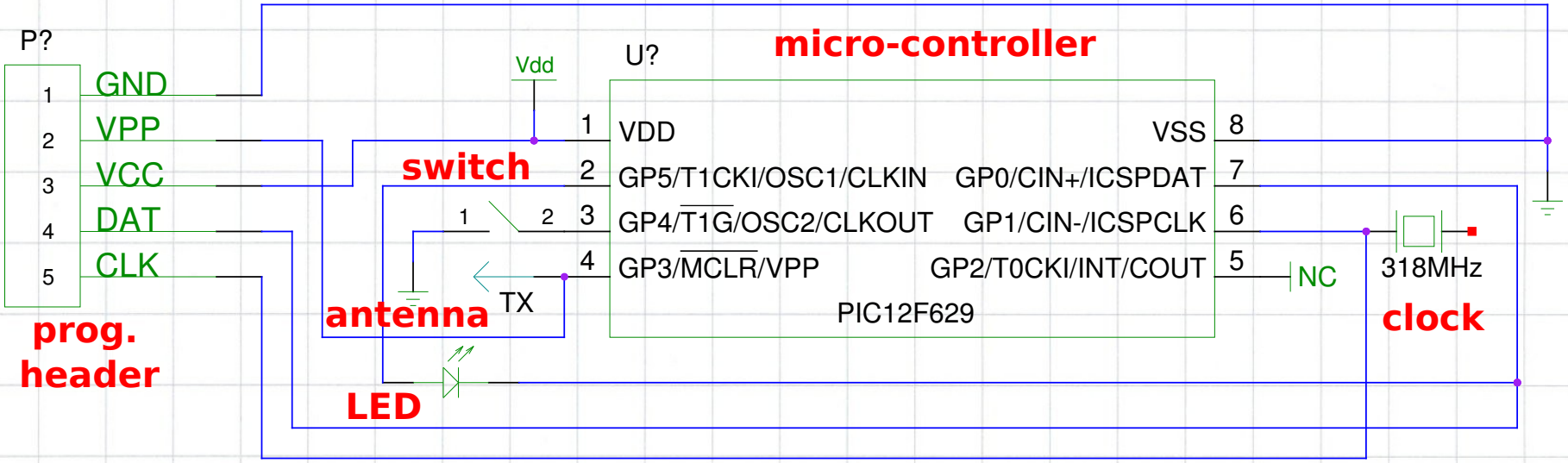


simple board with few components

follow the traces and use continuity test on multi-meter

3 - MegaCode cloning

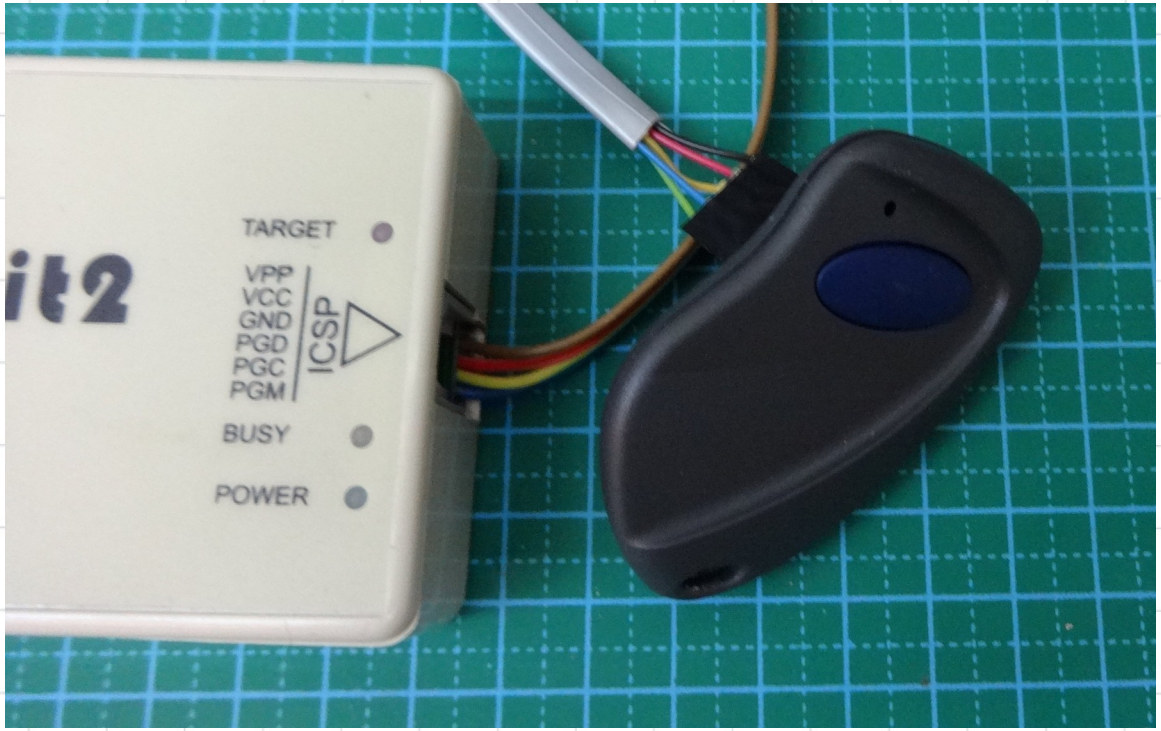
figure out the schematic



find which peripheral is connected to which pin required to start programming

3 - MegaCode cloning

implement the firmware

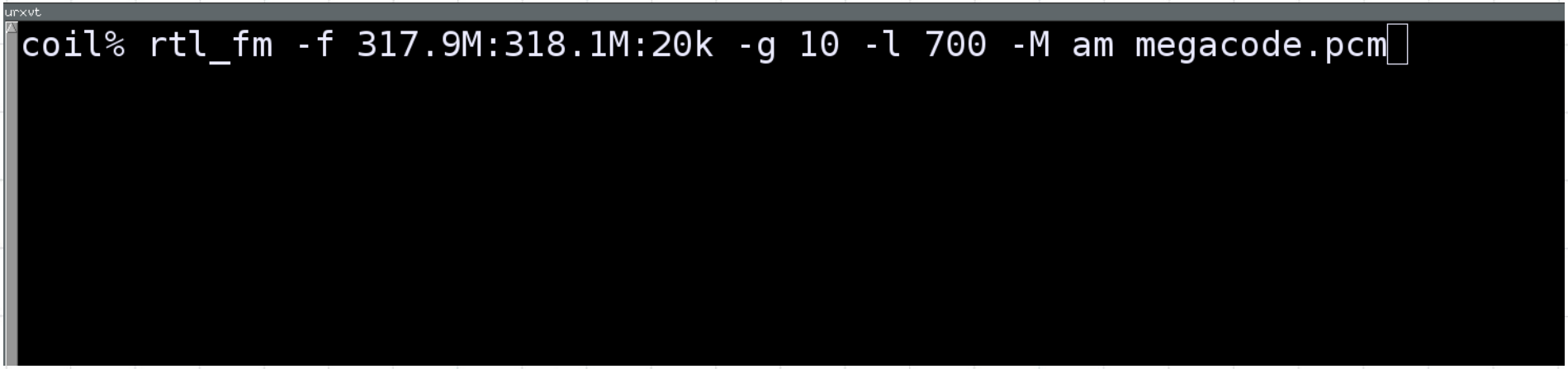


125 lines of code firmware

flash using PICkit2 programmer

4 - MegaCode collector

SDR + laptop is not practical



rtl_fm AM demodulation uses a narrow bandwidth

GNU Radio flow graphs are too advanced, antenna not ideal

my laptop battery only hold 30 min, and I use it every day

4 - MegaCode collector

buy receiver

amazon Try Prime | Your Amazon.com | Today's Deals | Gift Cards | Sell | Help

Shop by Department | Search | All | linear megacode receiver channel

1-16 of 83 results for "linear megacode receiver channel"

Show results for

Tools & Home Improvement
- Gate Hardware
- Garage Door Openers
- Garage Doors

Electronics
- Home Security Systems

+ See All 7 Departments

Refine by

International Shipping
- Ship to Germany

Eligible for Free Shipping

Linear MegaCode Plug-In Receiver, 1-Channel (DNR00100)
by Linear

$21.44
Only 7 left in stock - order soon.

More Buying Choices
$20.00 new (11 offers)

★★★★☆ 14

Product Features
MegaCode 1-Channel 110V Receiver

Electronics: See all 36 items

Linear MegaCode Receiver, 1-Channel (DNR00071)
by Linear

$27.50 ~~$29.95~~
Only 1 left in stock - order soon.

More Buying Choices
$13.02 new (12 offers)
$12.95 used (1 offer)

★★★★☆ 2

Product Features
Codes: 1,000,000+ (*MegaCode* format)

Electronics: See all 36 items

I prefer the ones not connected on mains
it's less hazardous

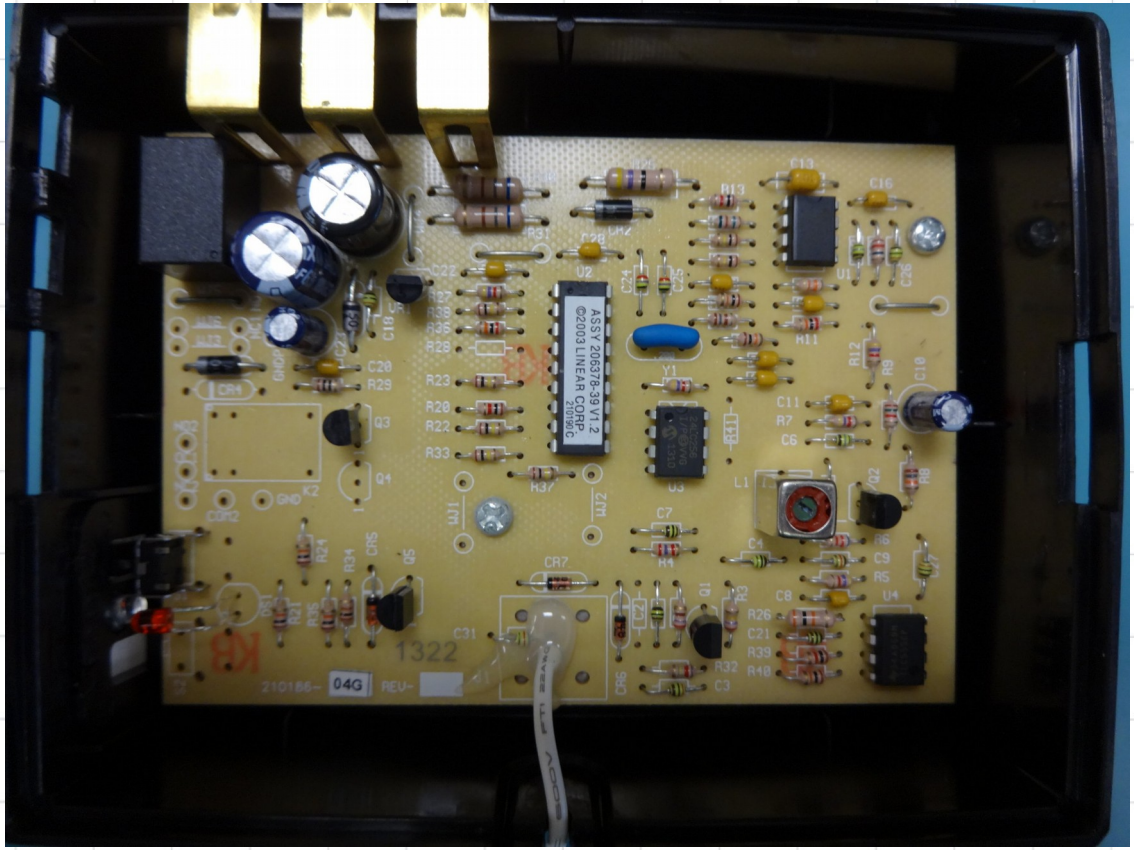
4 - MegaCode collector

get device

and tear it down

4 - MegaCode collector

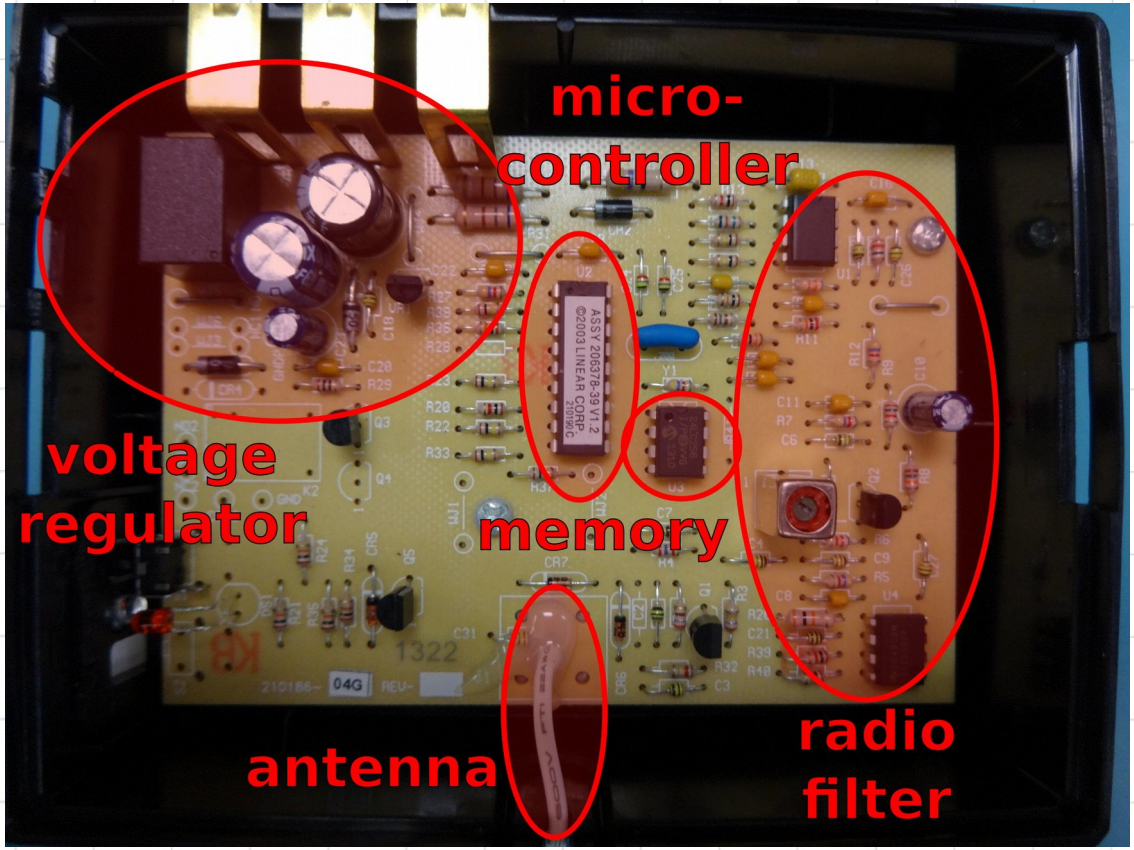
simple board



through hole components, easy to probe

4 – MegaCode collector

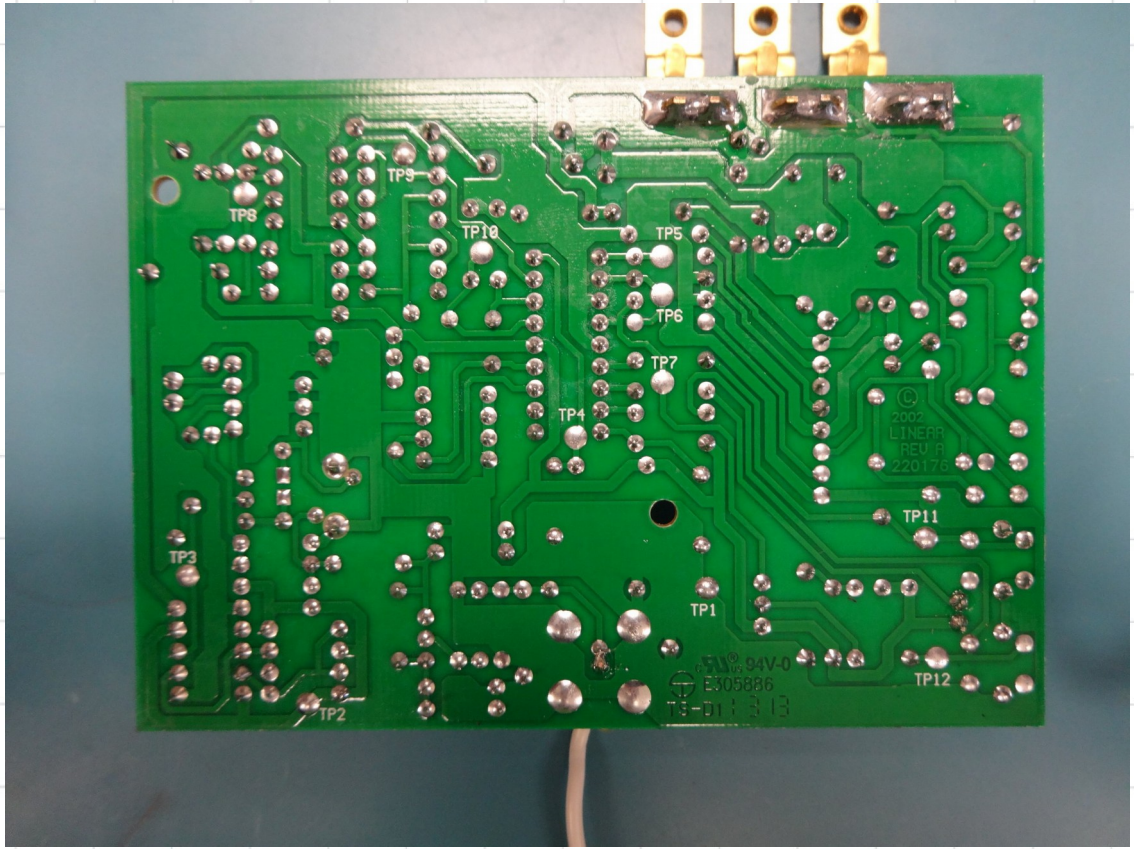
identify components



few components

4 - MegaCode collector

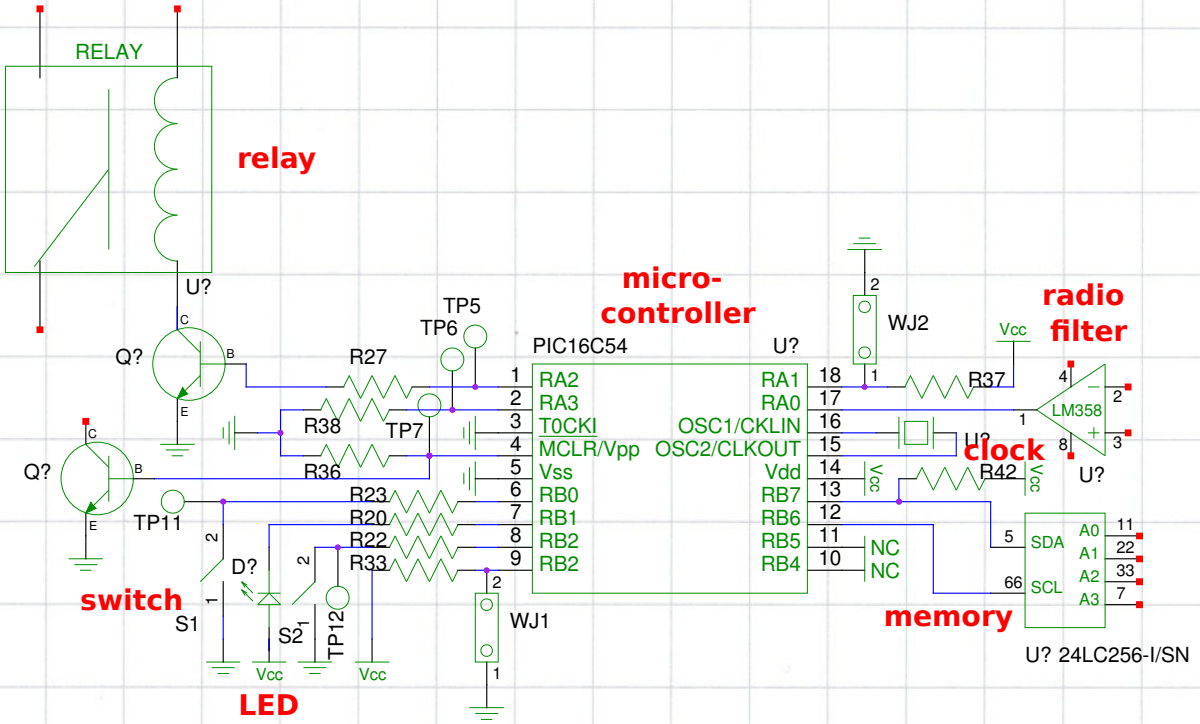
simple board



single layer, easy to trace connections

4 - MegaCode collector

reverse board

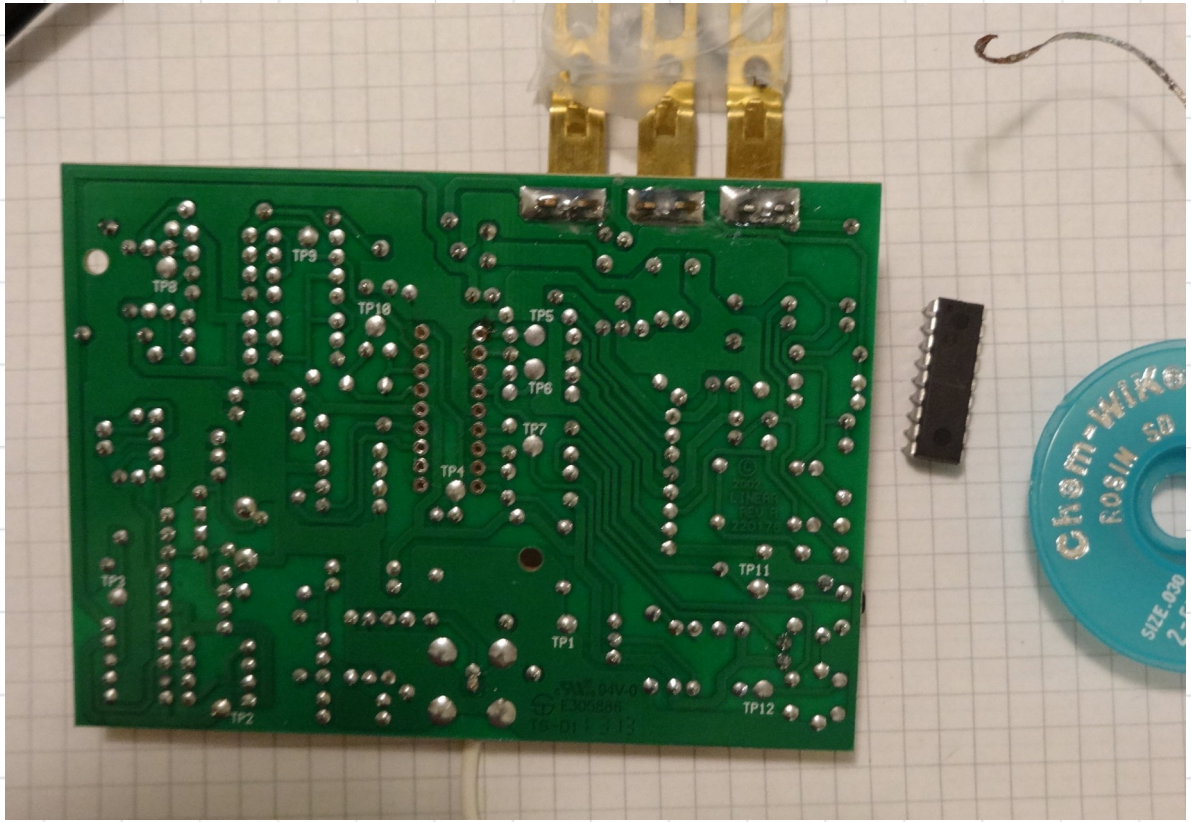


simple schematic, essential before implementing

Microchip PIC16C54 micro-controller, one time programmable

4 - MegaCode collector

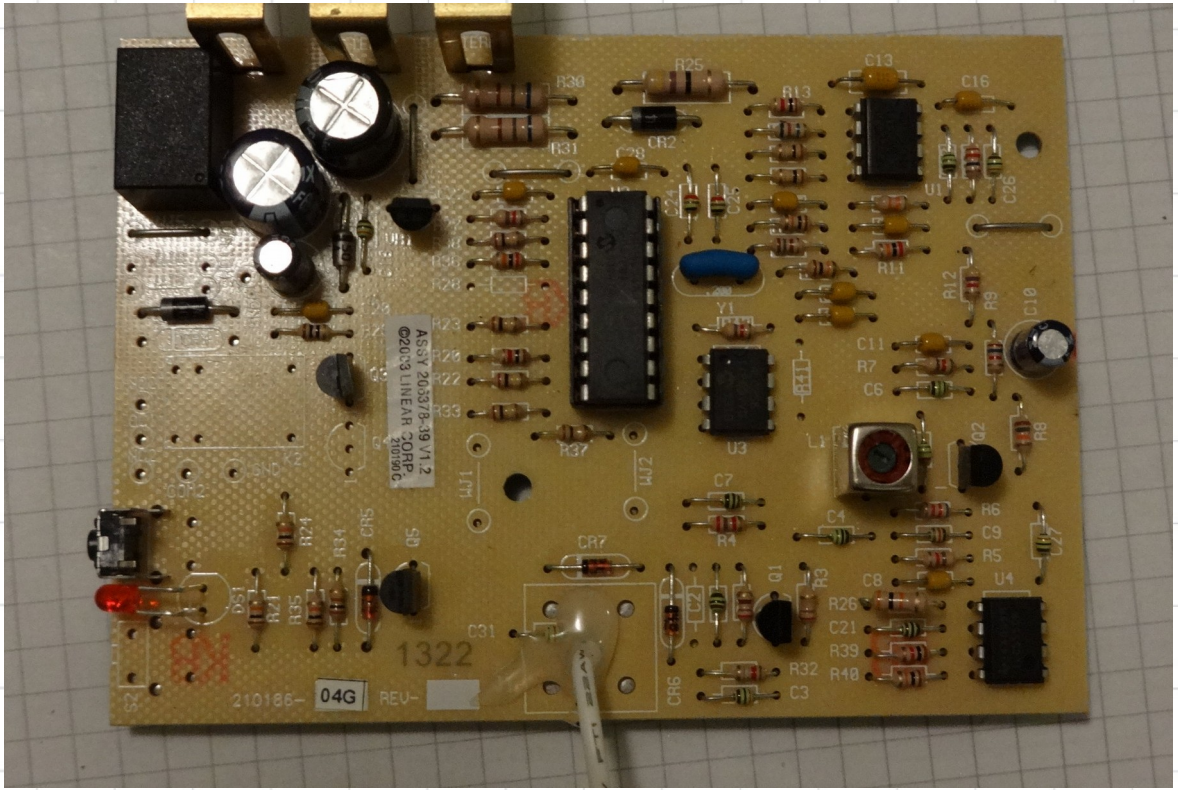
remove micro-controller



use solder wick or a vacuum pump

4 - MegaCode collector

implement decoder



444 lines of code firmware

4 - MegaCode collector

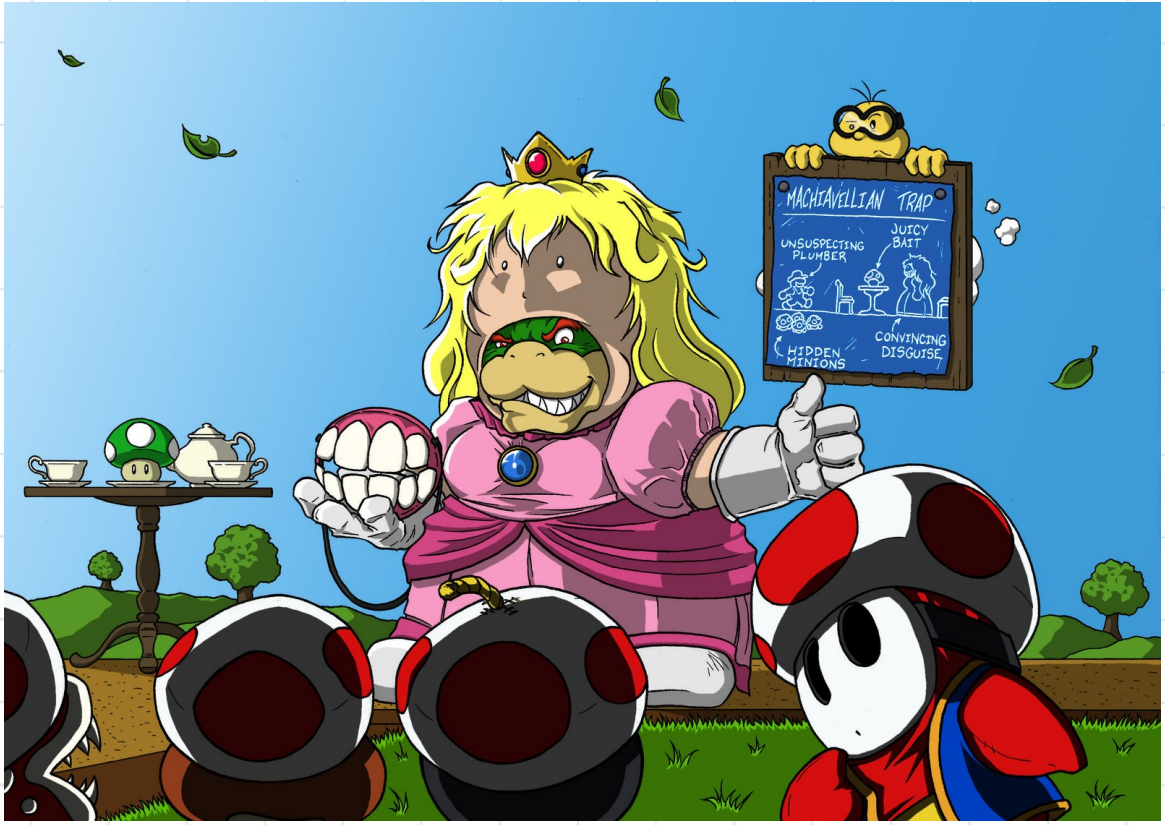
record codes

park near garage entrance

range: ~20m omnidirectional

4 - MegaCode collector

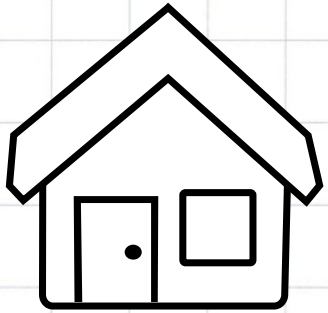
impersonation issue

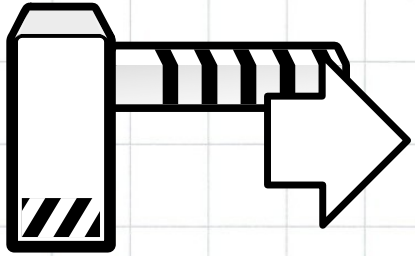


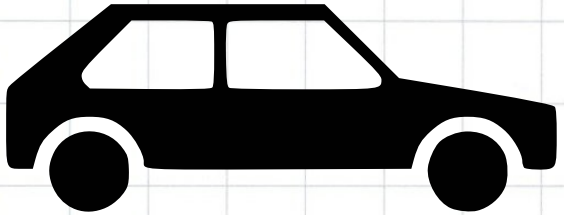
security entry logs are not valid any more

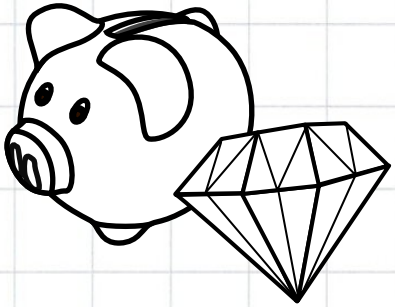
4 - MegaCode collector

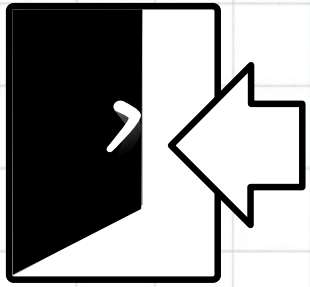
privacy issue











resident goes to work

robber also goes to work

4 - MegaCode collector

get higher privileged access code

enjoy hot tub until the security guard kicks you out (22:00)

record his code when he enters the pool area

4 - MegaCode collector

get higher privileged access code

code works on all buildings

even for the pool after 22:00

and the surveillance room next to the pool

4 - MegaCode collector

reverse which bits are relevant

```
[kevredon@dennou 318LPW1K-L]$ ./bit_change.rb
original code: 0x9a4ac6
bit flip 1, did 0x9a4ac7 work (enter=yes)?
bit flip 2, did 0x9a4ac4 work (enter=yes)? #
bit flip 3, did 0x9a4ac2 work (enter=yes)? #
bit flip 4, did 0x9a4ace work (enter=yes)?



bit flip 5, did 0x9a4ad6 work (enter=yes)?
bit flip 6, did 0x9a4ae6 work (enter=yes)?
bit flip 7, did 0x9a4a86 work (enter=yes)?
bit flip 8, did 0x9a4a46 work (enter=yes)?
bit flip 9, did 0x9a4bc6 work (enter=yes)?
bit flip 10, did 0x9a48c6 work (enter=yes)?
bit flip 11, did 0x9a4ec6 work (enter=yes)?
bit flip 12, did 0x9a42c6 work (enter=yes)?
bit flip 13, did 0x9a5ac6 work (enter=yes)?

bit flip 14, did 0x9a6ac6 work (enter=yes)?
bit flip 15, did 0x9a0ac6 work (enter=yes)?
bit flip 16, did 0x9acac6 work (enter=yes)?
bit flip 17, did 0x9b4ac6 work (enter=yes)?
bit flip 18, did 0x984ac6 work (enter=yes)?
bit flip 19, did 0x9e4ac6 work (enter=yes)?
bit flip 20, did 0x924ac6 work (enter=yes)?
bit flip 21, did 0x8a4ac6 work (enter=yes)?

bit flip 22, did 0xba4ac6 work (enter=yes)?
bit flip 23, did 0xda4ac6 work (enter=yes)? 0x9a4ac6 1xxxxxxxxxxxxxxxxxxx11x
```

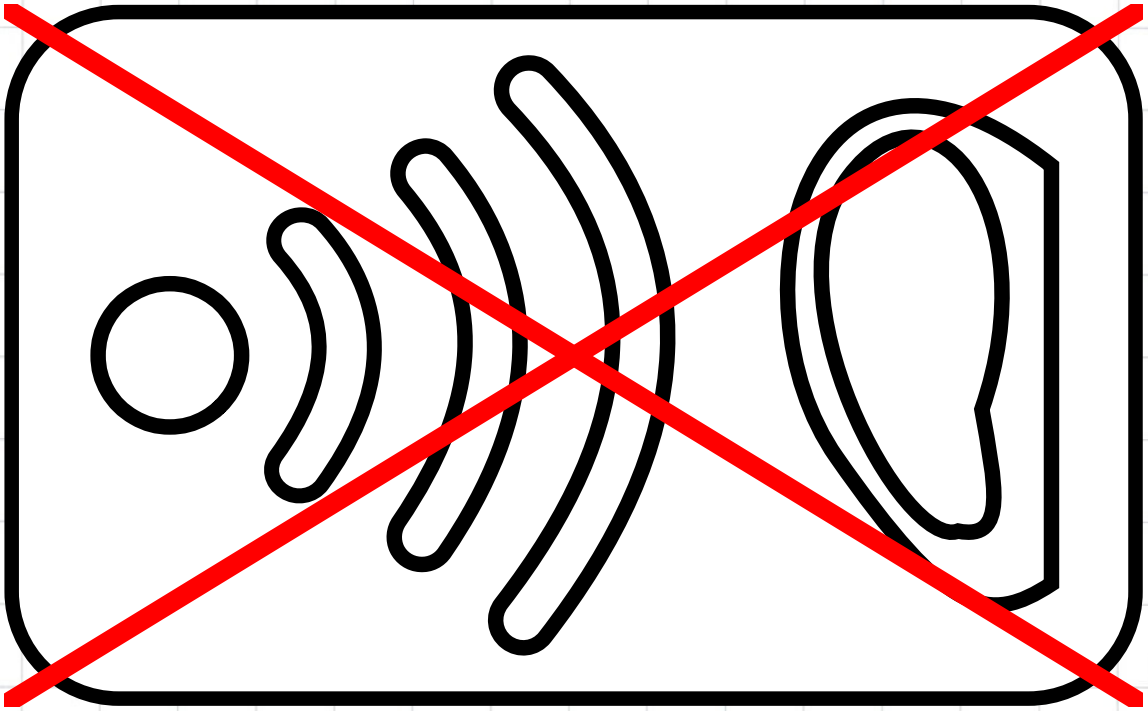
use a working code, flip single bit, test code using remote

out of 24 bits only 15 are relevant

with 1000+ residents brute forcing should not take long

5 - MegaConclusion

responsible disclosure



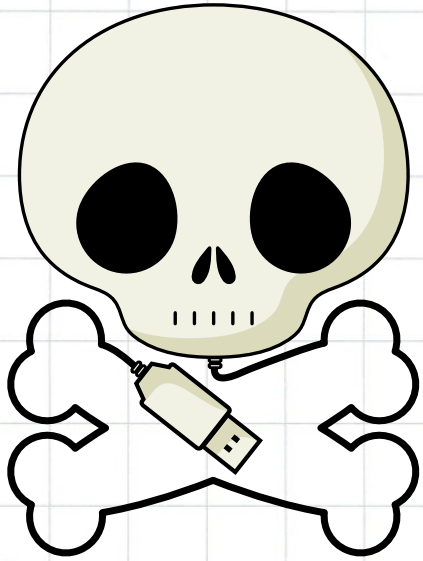
vendor contacted, but no response

easy counter-measure: rolling codes

5 - MegaConclusion

lessons learned

- reverse engineered a real security device
- improve intelligence and social skills
- program a micro-controller
- used software defined radio
- solder and de-solder chips



MEGACODE® to facility gates

questions?

contact: kingkevin@cuvoodoo.info

videos with more technical details:
https://www.cuvoodoo.info/?post_type=podcast&p=69
https://www.cuvoodoo.info/?post_type=podcast&p=71

pictures are documentation:
https://wiki.cuvoodoo.info/doku.php?id=megacode

source code:
https://git.cuvoodoo.info/kingkevin/megacode