Toniebox 101

An audio player not only for kids

Moritz

BornHack 2024

Disclaimer

- there was an entertaining German talk at **37C3** https://media.ccc.de/v/37c3-11993-toniebox_reverse_engineering
- who saw this: no news here

What is it?

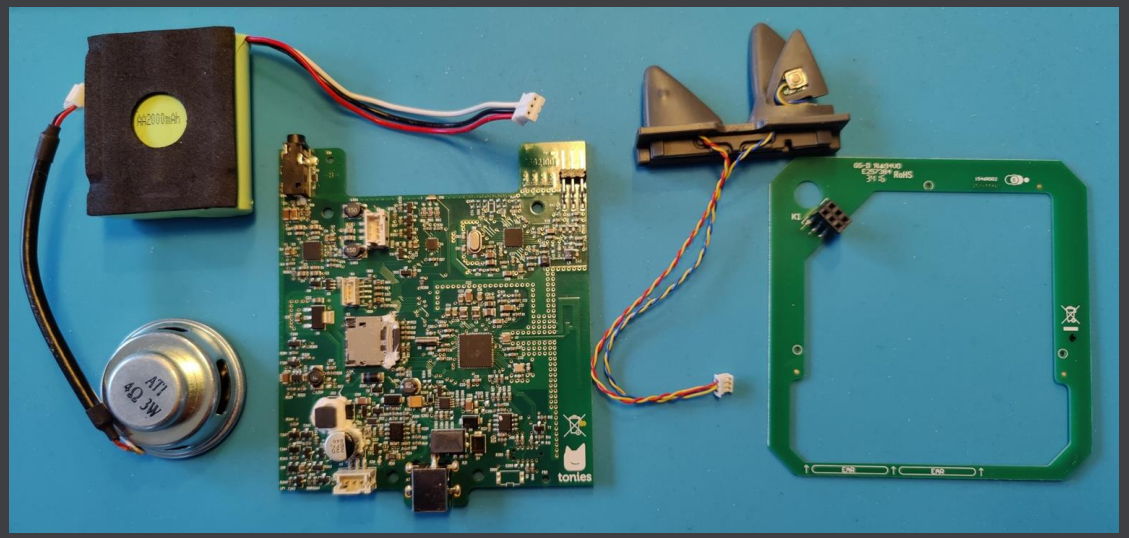
- a cube-shaped digital audio device designed for children
- NFC figures used for the content
- no display
- ears for volume control
- simple and easy to use for kids
- currently available in DE, AT, CH, UK, IR, US, FR, CA
- rest of Europe online

Why?

- curiosity
- dependency on yet another cloud service
- walled garden
- nosiness of the manufacturer
- technical reasons
  - works only with original figures
  - artificial 90m limit for own content
  - own content only with expensive creative tonies

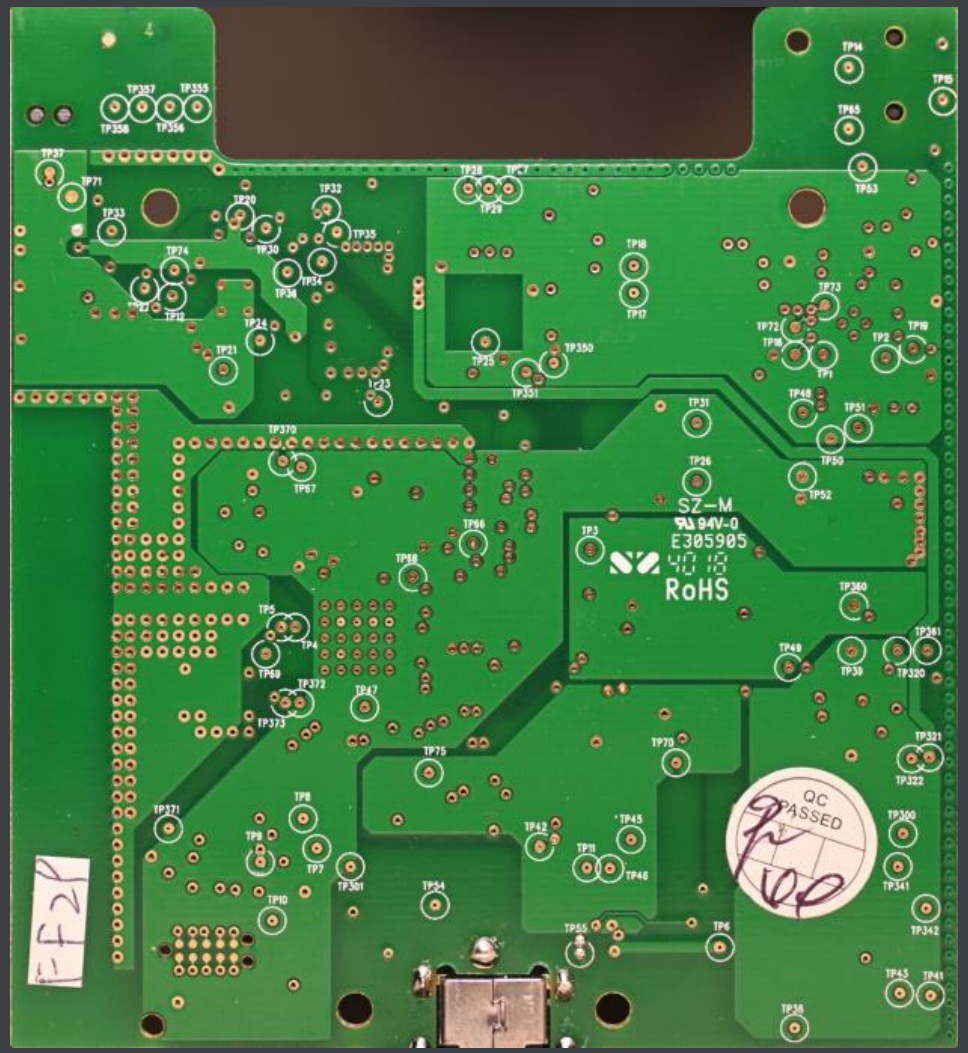
Components

- speaker
- battery pack (NiMH)
- PCB
- ears with integrated buttons
- antenna



Toniebox PCB

- four layers
- components only on top layer
- 82 testpoints
- WiFi antenna



FEATURE CREEP

Microcontroller (TI CC3200)

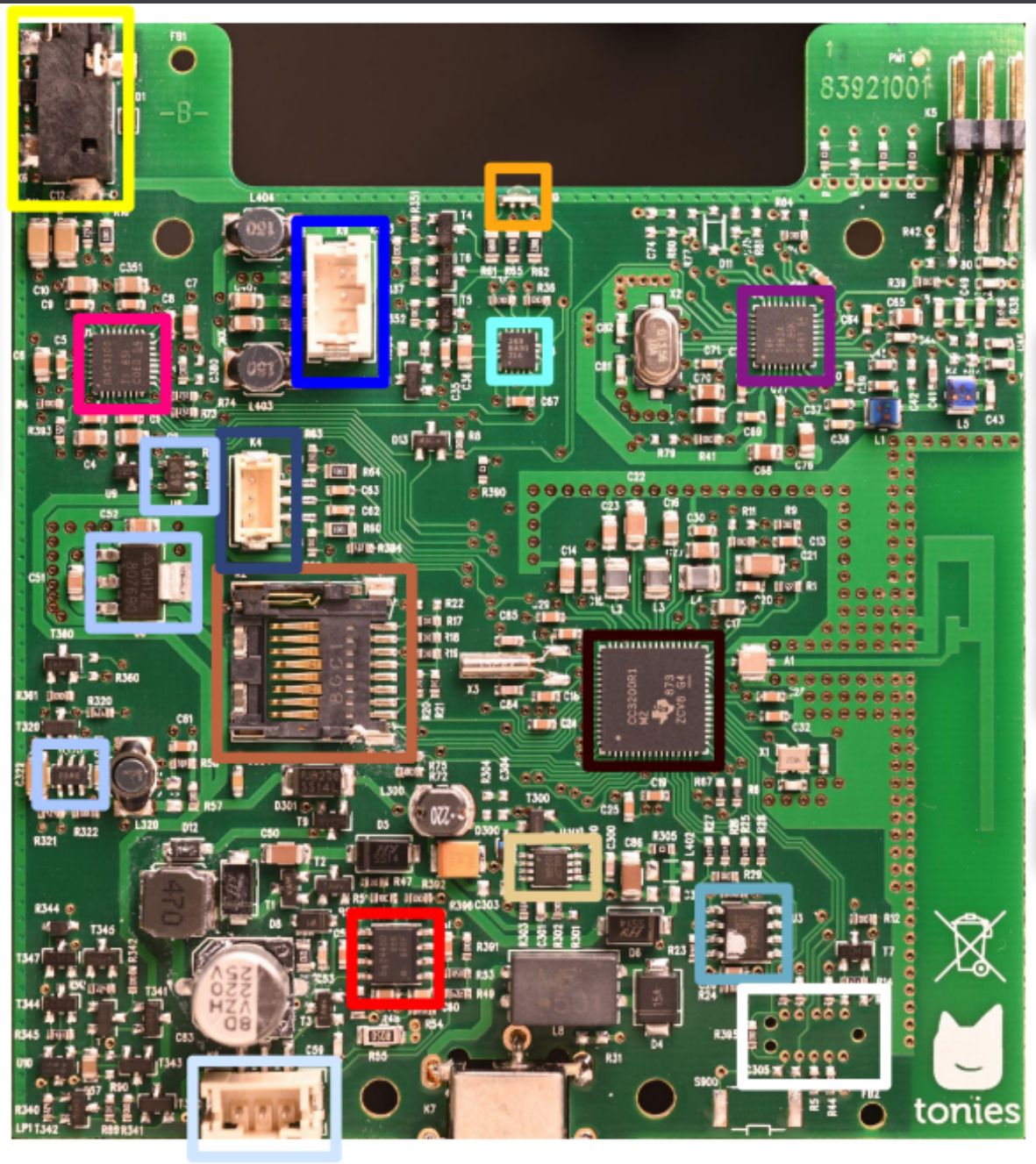
RFID IC (TRF7962A)

MEMS-accl.sensor (MMA8451QT)

Audio DAC (TLV320DAC3100)

Serial flash (IS25LQ032B)

SD-Card



Charge management (BQ24400)

DC/DC step down (LM3485MM)

LDOs/power supplies

RGB LED

Audio out

Battery

Ears

Speaker

Debug IF (Tag Connect)

FEATURE CREEP

Toniebox Hardware

- three different uC over the years
  - TI CC3200
  - TI CC3235 (US)
  - Espressif ESP32-S3

CC3200

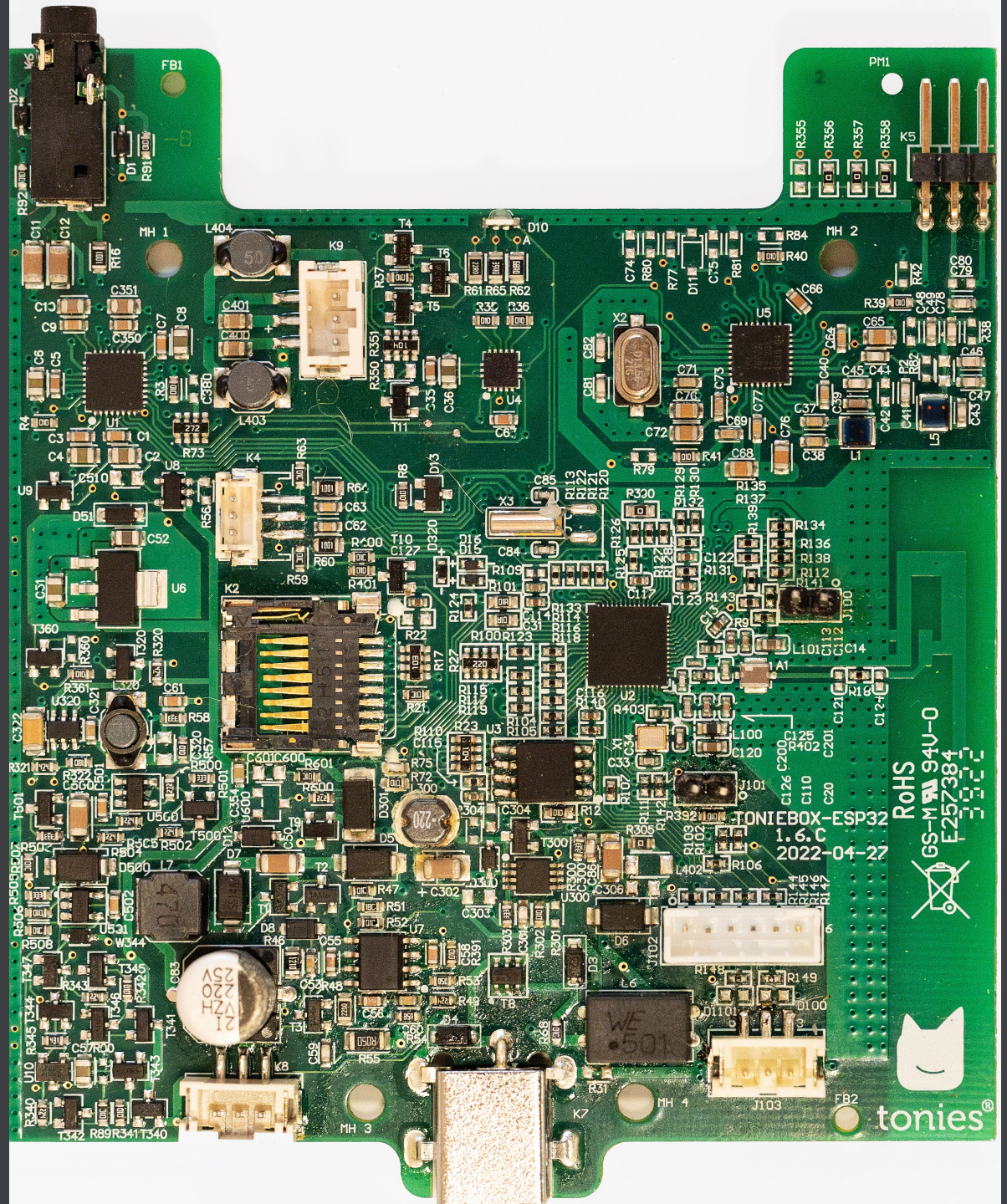
- pretty widespread, mostly older boxes
- debug interface: tag connect
- flash is unencrypted and unsigned
- `cc3200tool` for reading and writing with tag connect adapter
- custom firmware (Hackiebox)
- custom bootloader (HackieboxNG)

CC3235

- for US market
- rare in Europe
- debug interface: tag connect, but likely locked
- access to flash possible, but needs SOP8 clamps
- content partially encrypted
  - certificates unencrypted
  - firmware signed and encrypted
- `cc32tool` for manipulating the flash dump

ESP32

- latest version, new boxes
- debug interface `UART`, common for esp32
- accessible with `esptool`
- flash unencrypted and unsigned
- custom firmware (PoC)
  - Hackiebox ESPuino port
  - TeddyBox



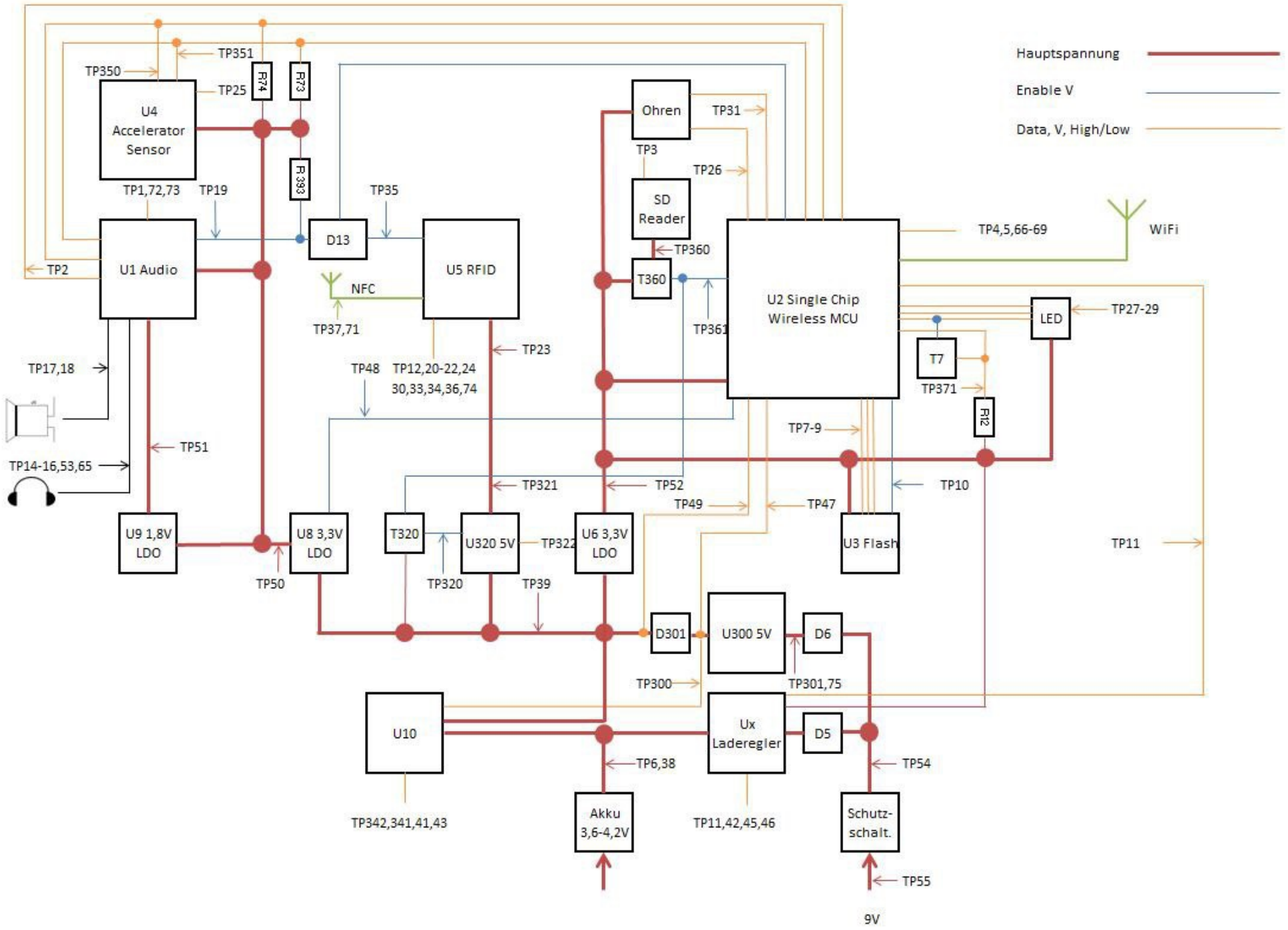
FEATURE CREEP

Schematic/Block Diagram

- basic KiCad schematic available on GitHub
- testpoint table https://github.com/toniebox-reverse-engineering/toniebox-pcb#testpoints
- 82 testpoints
  - at least connections specified
  - 50 commented

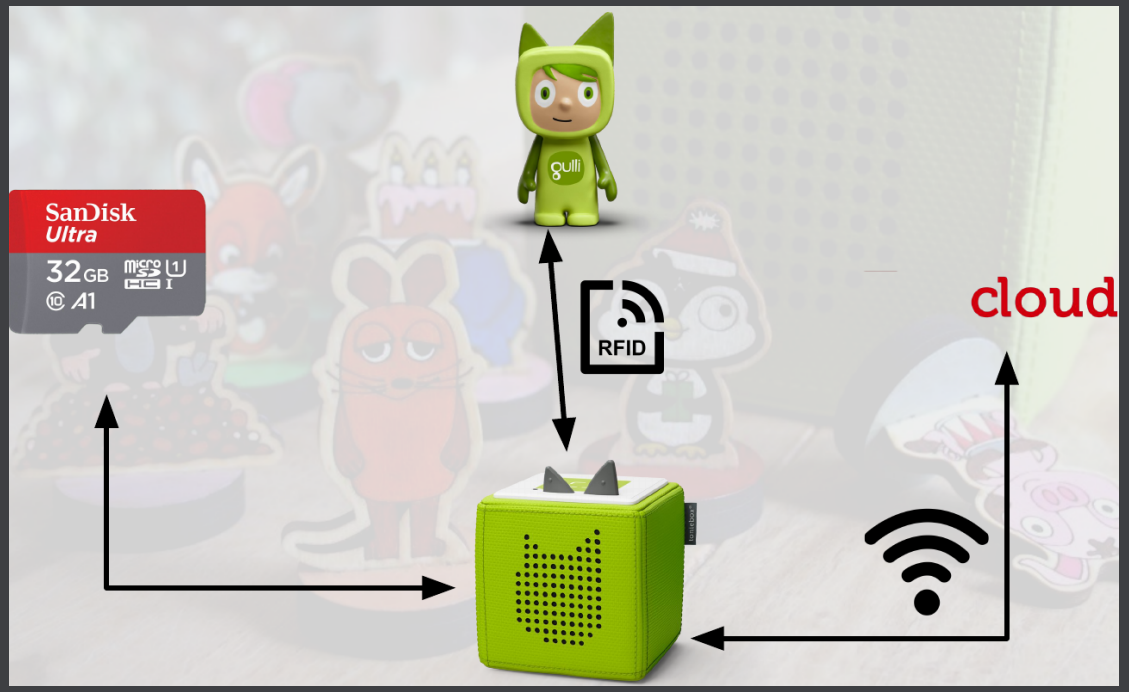
README

TP41	Circuit next to U10	0V w/o battery, ~ bat. voltage w/ battery; output of T344; connected to U10; controls T343, T342, T340
TP42	BQ24400 BAT input	
TP43	U10 /	battery voltage after R89; w/ battery: voltage < bat voltage; w/ power supply 3.8 – 4.4V; check TP38 if not ok
TP45	K8 pin 1/U7 pin 5 (TS)	temp sense; connected via R47 with BQ24400 and battery NTC.
TP46	BQ24400 TIMER PROGRAM	
TP47	U2 pin 8/output L300 via 1:1 voltage divider R75/R72	Supervising U300+circuitry; measured between D301 and L300; 50% voltage via divider R75/R72 to U2 pin 8
TP48	U2 pin 61/U8 ENABLE via R56 (10k pulldown)	U2 enables LDO U8 with GPIO6. If U8 is not working (TP50) check U8 at TP39
TP49	U2 pin 60	
TP50	U8 VOUT/U9 VIN/U1 IOVDD/U1 HPVDD/SPKVDD/AVDD	3V3 output of LDO U8, 1V8 input of LDO U9, T11, U4. 3V3 input U1; if not ok check TP48.
TP51	U9 VOUT/U1 DVDP	1V8 output of LDO U9. Feeds U1 at PIN 3; if not ok check ENABLE at TP50 and input voltage at TP39.
TP52	U6 VOUT 3V3/ U2 VIN IO1, VIN IO2, VIN DCDC ANA, VIN DCDC PA, VIN DCDC DIG, VD2 ANA2/ VCC for U3,T7, T360, T320, SV BQ24400 LED/ RGB LED	3V3 output LDO U6: feeds U2, U3, T360 (TP360), TP320, LED output of BQ24400 (TP11)


Hauptspannung
Enable V
Data, V, High/Low
U4 Accelerator Sensor
TP350
TP351
TP25
R74
R73
R393
TP1,72,73
TP19
TP35
U1 Audio
TP2
D13
NFC
TP37,71
U5 RFID
TP23
TP48
TP12,20-22,24 30,33,34,36,74
TP17,18
TP14-16,53,65
TP51
Ohren
TP31
TP3
TP26
SD Reader
TP360
T360
TP361
U2 Single Chip Wireless MCU
TP4,5,66-69
WiFi
LED
TP27-29
T7
TP371
R12
TP7-9
TP10
TP321
TP52
TP49
TP47
U3 Flash
TP11
U9 1,8V LDO
U8 3,3V LDO
T320
U320 5V
TP322
U6 3,3V LDO
TP50
TP320
TP39
D301
U300 5V
D6
TP300
TP301,75
U10
Ux Laderegler
D5
TP6,38
TP54
TP342,341,41,43
Akku 3,6-4,2V
TP11,42,45,46
Schutz-schalt.
TP55
9V

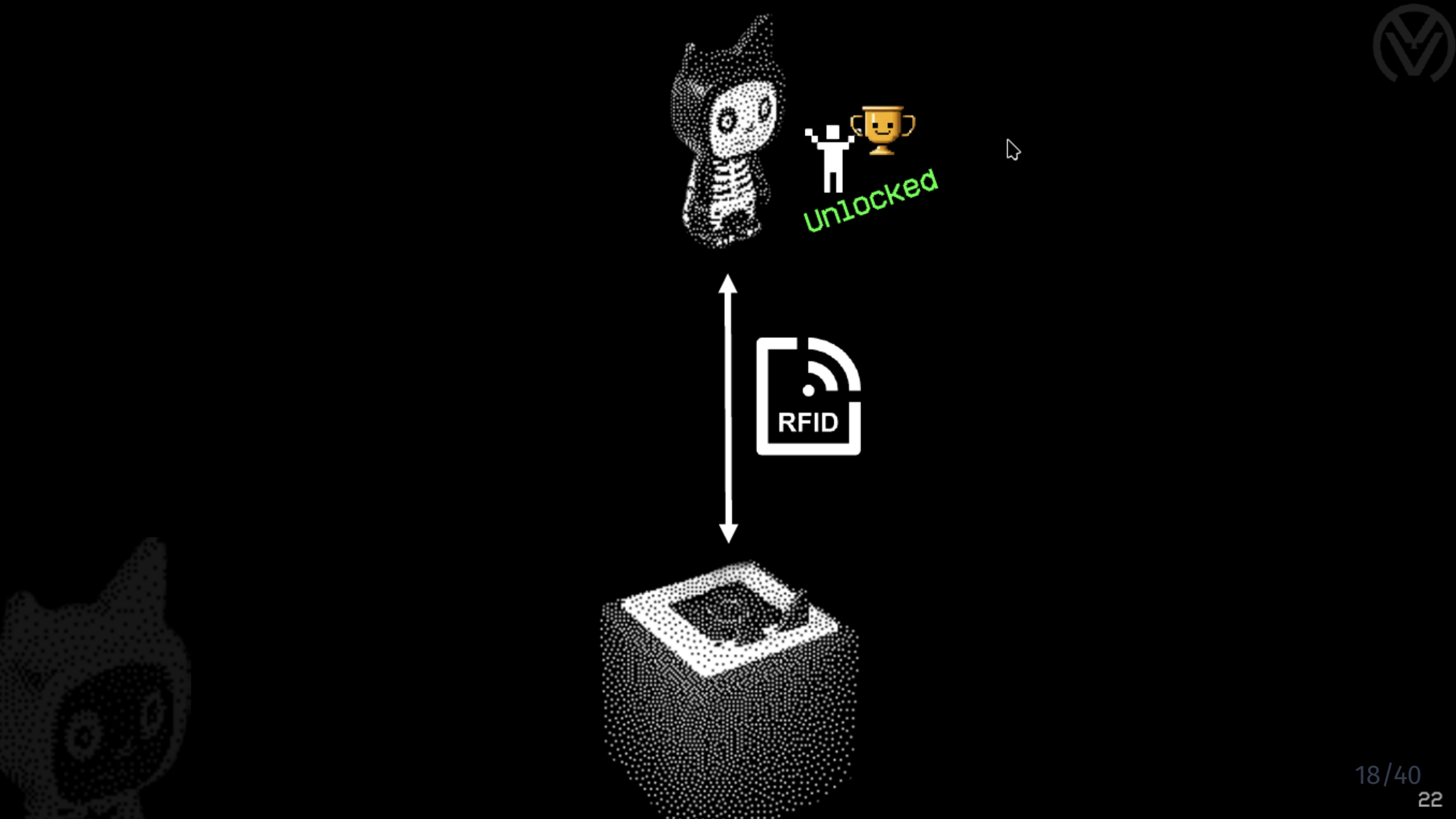
How does it all work?

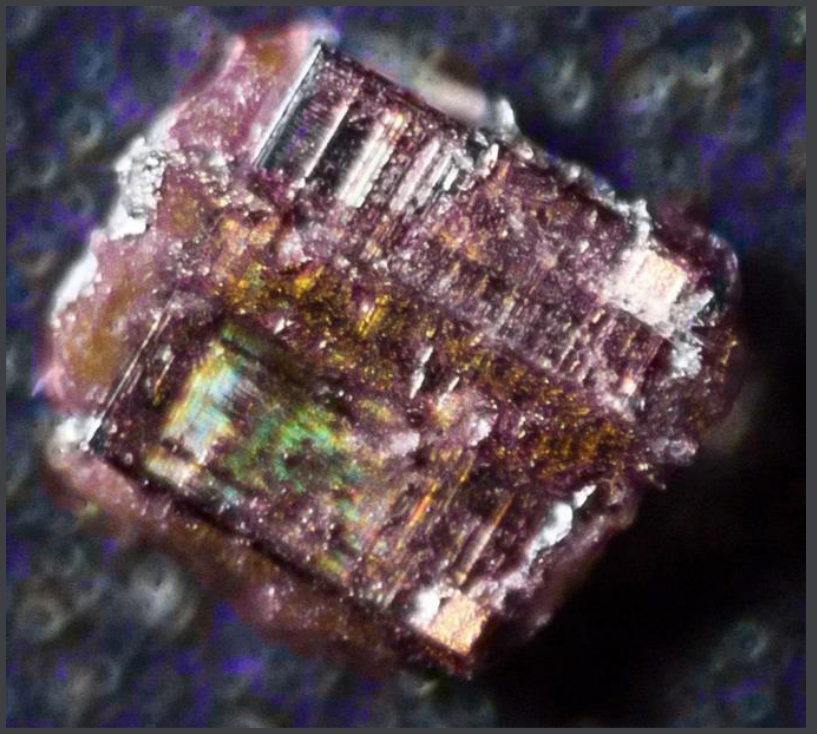
- put the Tonie on top
- read the `UID` from tag
- if there is no related content on the SD card
  - read tag memory
  - get audio content from cloud
  - write content to SD card
- play audio content



NFC

- NXP SLIX-L / ISO 15693
- privacy mode, will not reveal data, except `GET RANDOM NUMBER` and `SET PASSWORD`
- antenna made of coiled wire
- fake tags and clone tags exist
- custom tags are working
- Flipper Zero and Proxmark3 SLIX-L unlock and emulator added
- see https://www.g3gg0.de/rf/flipper-zero-got-iso15693-nfc-v-support for details (»this was some serious journey«)


Unlocked
RFID



FEATURE CREEP

How does the SD card content work?

- content filed in directories
- opus files with padding and `protobuf` header

Tonie Audio File (TAF)

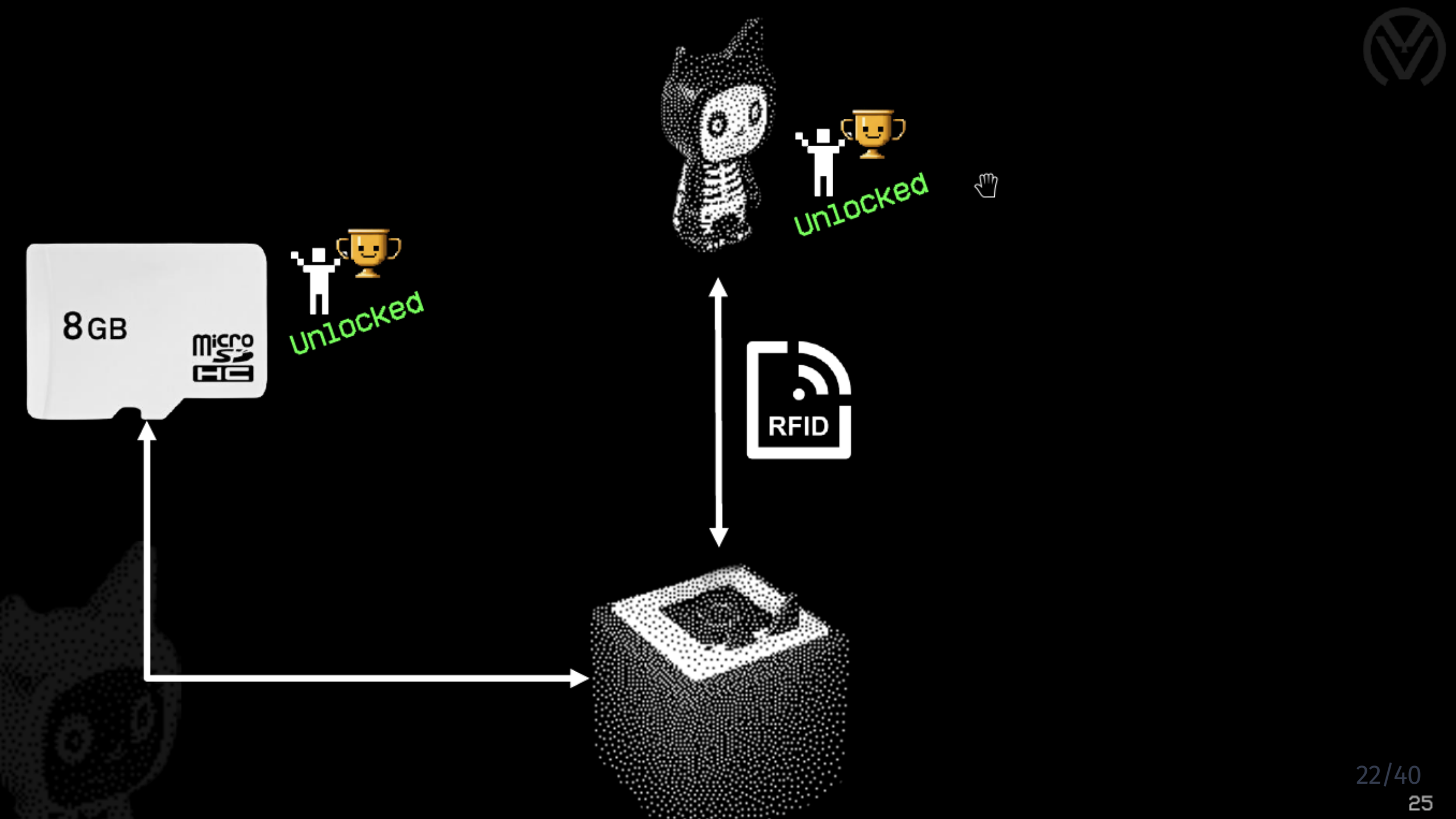
SD:\CONTENT\xxxxxxxx\500304E0

UUID[8]: E0040350xxxxxxxx
MEM[32]: 8008D512DED9F76F…8F252FDE

4k	TAF HEADER
4k	OGG/OPUS HEAD/PAGE
4k	OGG/OPUS PAGE
…	OGG/OPUS PAGE
	OGG/OPUS PAGE
	OGG/OPUS PAGE
	OGG/OPUS PAGE
	OGG/OPUS PAGE
	…

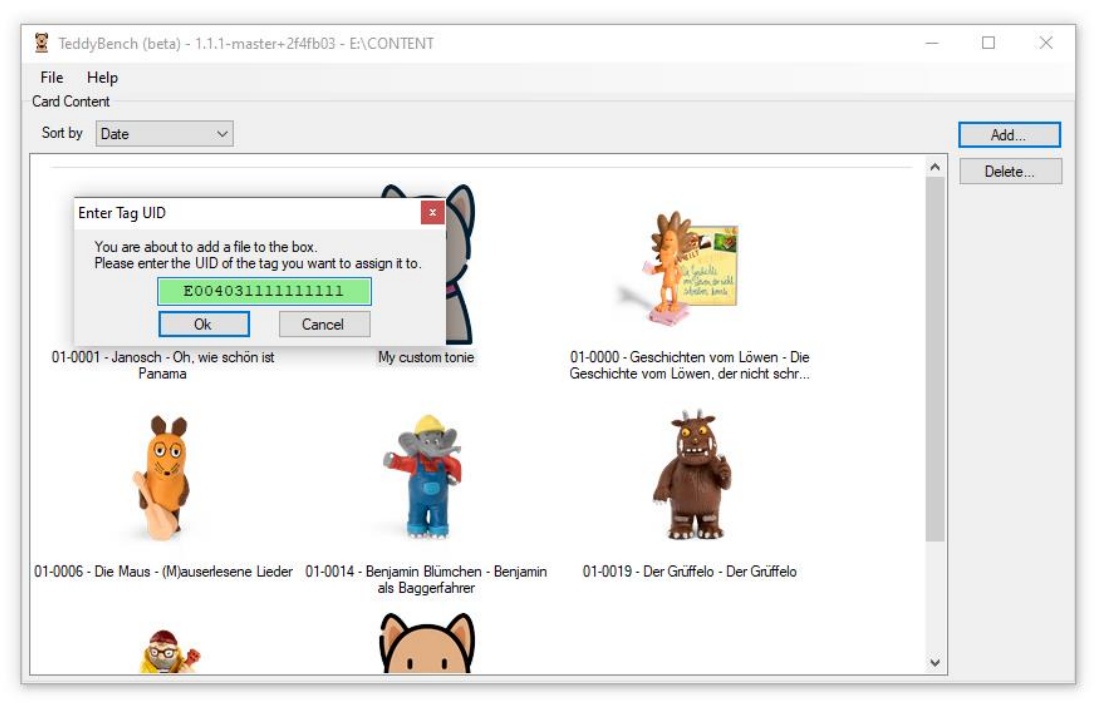
Protobuf coded:
bytes OGG SHA1 hash
uint64_t OGG size
uint32_t OGG audio id
uint32_t[] track / block map
bytes padding

OggS page
OPUS packet
OPUS packet
…
OPUS packet
padding


8GB
micro SD HC
Unlocked
Unlocked
RFID

Teddybench (level: easy)

- software for manage content on the SD card
- converts MP3 to OPUS
- displays content of SD card based on a list of 1100 tonies (`tonies.json`)
- cons:
  - box needs to be offline mode
  - custom tags are difficult to obtain

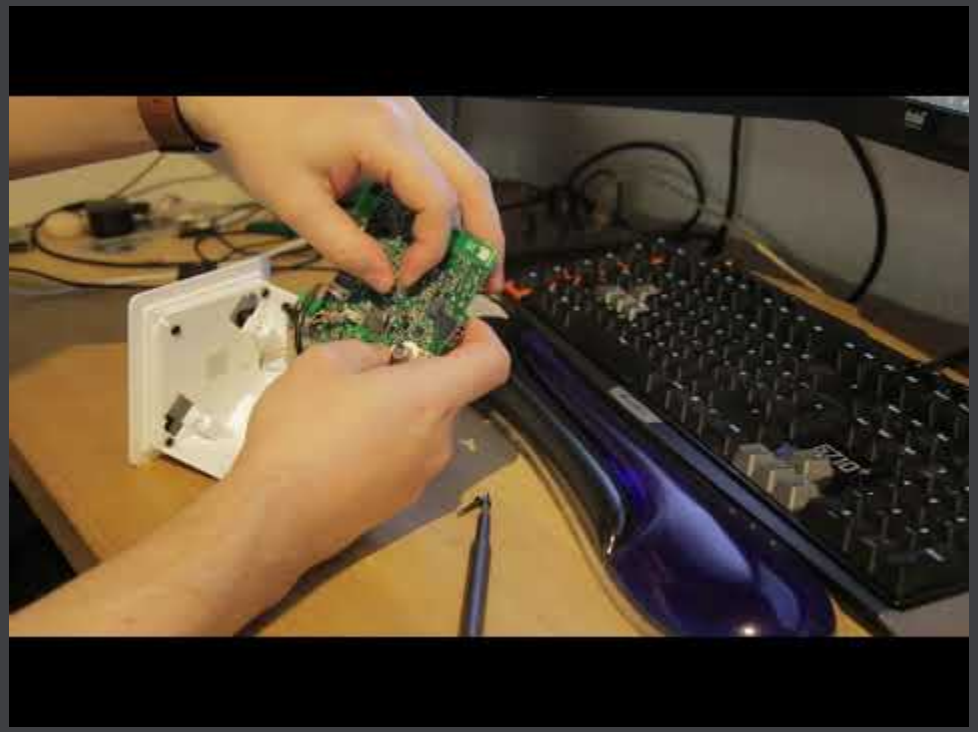


tonies.json

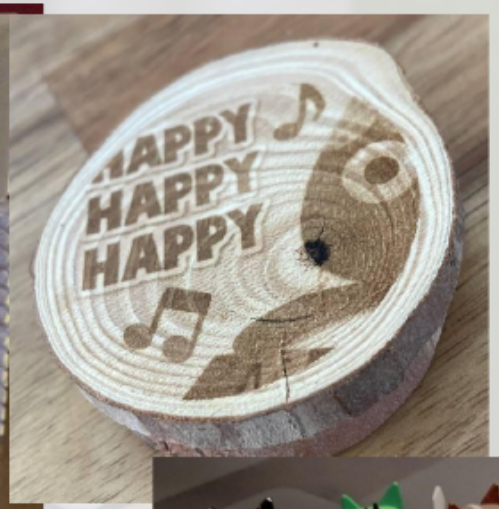
	A	B	C	D
1	article	series	series-id	episode
2	01-0000	Geschichten vom Löwen		Die Geschichte vom Löwen, der nicht schreiben konnte
3	01-0001	Janosch	janosch	Oh, wie schön ist Panama
4	01-0002	Die Olchis	die-olchis	Die Olchis auf Geburtstagsreise
5	01-0003	Die Olchis	die-olchis	Die Olchis und der schwarze Pirat
6	01-0004	Die Olchi-Detektive		Das Erbe der Piraten
7	01-0005	Der kleine Rabe Socke	der-kleine-rabe-socke	Alles erlaubt?
8	01-0006	Maus	maus	(M)auserlesene Lieder
9	01-0007	Das Sams	das-sams	Eine Woche voller Samstage
10	01-0008	Das Sams		Am Samstag kam das Sams zurück
11	01-0009	Bobo Siebenschläfer	bobo-siebenschlaefer	Bobos Ausflug zum Spielplatz
12	01-0010	Conni		Conni kommt in den Kindergarten / Conni macht das Seepferdche
13	01-0011	Conni		Conni auf dem Bauernhof / Conni und das neue Baby
14	01-0012	Bibi Blocksberg	bibi-blocksberg	Hexen gibt es doch
15	01-0013	Benjamin Blümchen	benjamin-bluemchen	Der Zoo-Kindergarten
16	01-0014	Benjamin Blümchen	benjamin-bluemchen	Benjamin als Baggerfahrer
17	01-0018	Kleiner Eisbär		Lars, lass mich nicht allein! / Lars und der Angsthase
18	01-0019	Der Grüffelo		Der Grüffelo
19	01-0020	Die Olchis		Die Olchis werden Fußballmeister
20	01-0021	Unter meinem Bett	unter-meinem-bett	Unter meinem Bett 1
21	01-0022	Janosch	janosch	Ich mach dich gesund, sagte der Bär
22	01-0023	Der kleine Drache Kokosnuss	der-kleine-drache-kokosnuss	Hörspiel zur TV-Serie 01
23	01-0024	Bobo Siebenschläfer	bobo-siebenschlaefer	Bobo feiert Kindergeburtstag
24	01-0025	Teufelskicker	teufelskicker	Moritz macht das Spiel!
25	01-0027	Ritter Rost	ritter-rost	Die Zauberinsel


```
{
    "article": "2000001824",
    "data": [
        {
            "series": "Käpt'n Sharky",
            "episode": "Die geheimnisvolle Nebelinsel",
            "release": 1551398400,
            "language": "de-de",
            "category": "audio-play",
            "runtime": 0,
            "age": 4,
            "origin": "tunes",
            "image": "https://cdn.tonies.de/o/images/1_95a23d40b78d9ad5152af512804 5bef9395ab72076b5572861a91c46/3_1XCfMnrC1f8RxnpX/kapt_n_shar
            "sample": null,
            "web": "https://tonies.com/de-de/audio-content/kaept-n-sharky/kaptn-sharky-die-geheimnisvolle-nebelinsel/",
            "shop-id": "711a9065-4f36-4393-ad08-d4e430181418",
            "track-desc": [
                "Sharkys Piratenlied 13",
                "Die Flaschenpost (Teil 1)",
                "Die Flaschenpost (Teil 2)",
                "Die Flaschenpost (Teil 3)",
                "Auf zu neuen Abenteuern",
                "Piratenmeisterdichter",
                "Die Insel im Nebel (Teil 1)",
                "Die Insel im Nebel (Teil 2)",
                "Die Insel im Nebel (Teil 3)",
                "Die Insel im Nebel (Teil 4)",
                "In der Grotte (Teil 1)",
                "In der Grotte (Teil 2)",
                "In der Grotte (Teil 3)",
```

Removing the SD card




#28


HAPPY
HAPPY
HAPPY


Liederfibel

How does the cloud work

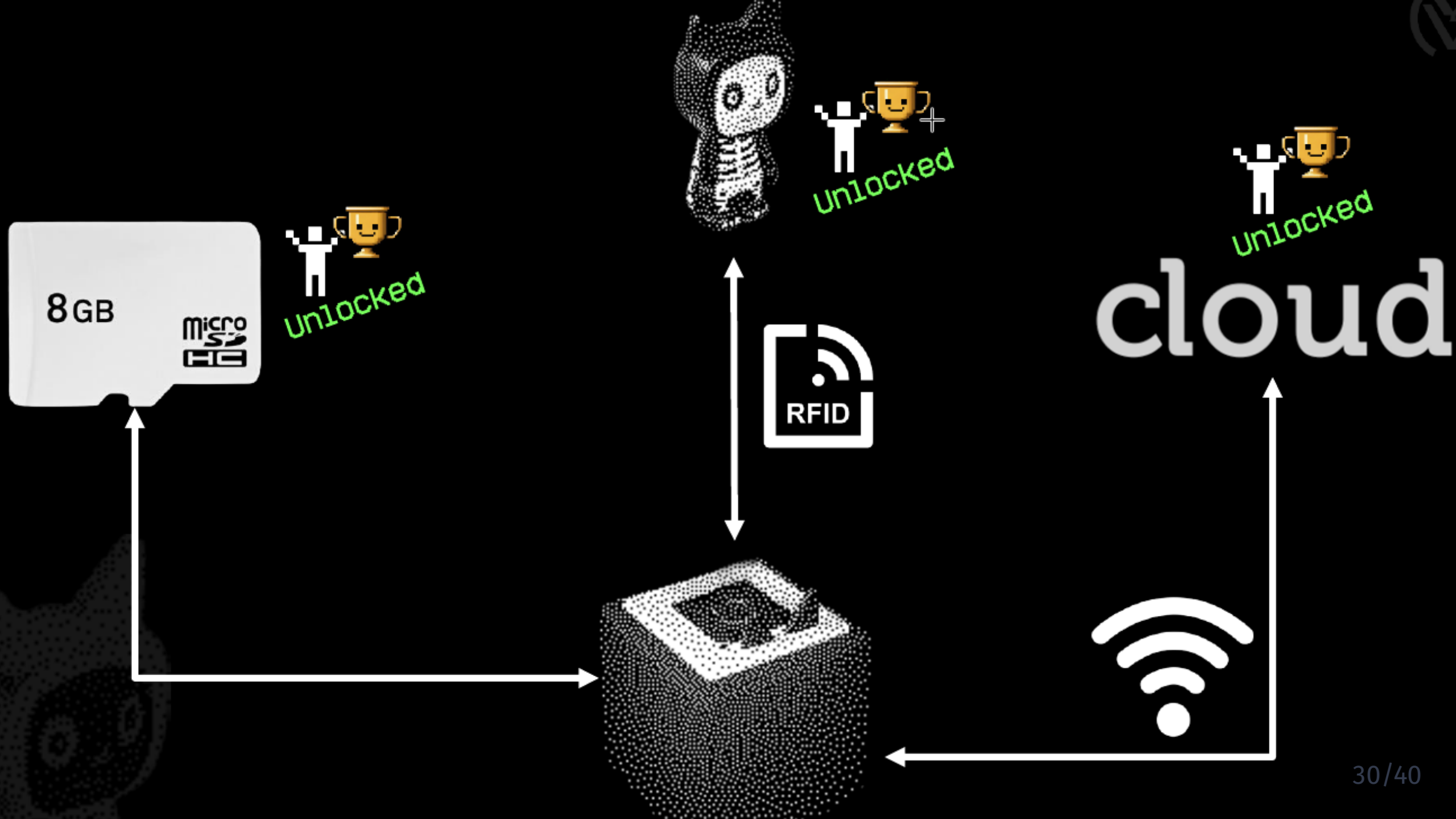
- we put some effort into figuring out how the cloud works
- result in our wiki on GitHub: https://toniebox-reverse-engineering.github.io/docs/wiki/general/protocol-analysis/

Cloud-API

API	Parameter	Antwort
https://prod.de.tbs.toys/ /v1/time		Unix-Zeit
/v1/ota	/<file_id>?cv=<time>	Firmware
/v1/claim	/<UID-rev>	
/v1/content		Tonie Audio File
/v2/content		
GET /v1/log		
GET+Auth /v1/cloud-reset		<json>
POST /v1/freshness-check	<protobuf>	<protobuf>

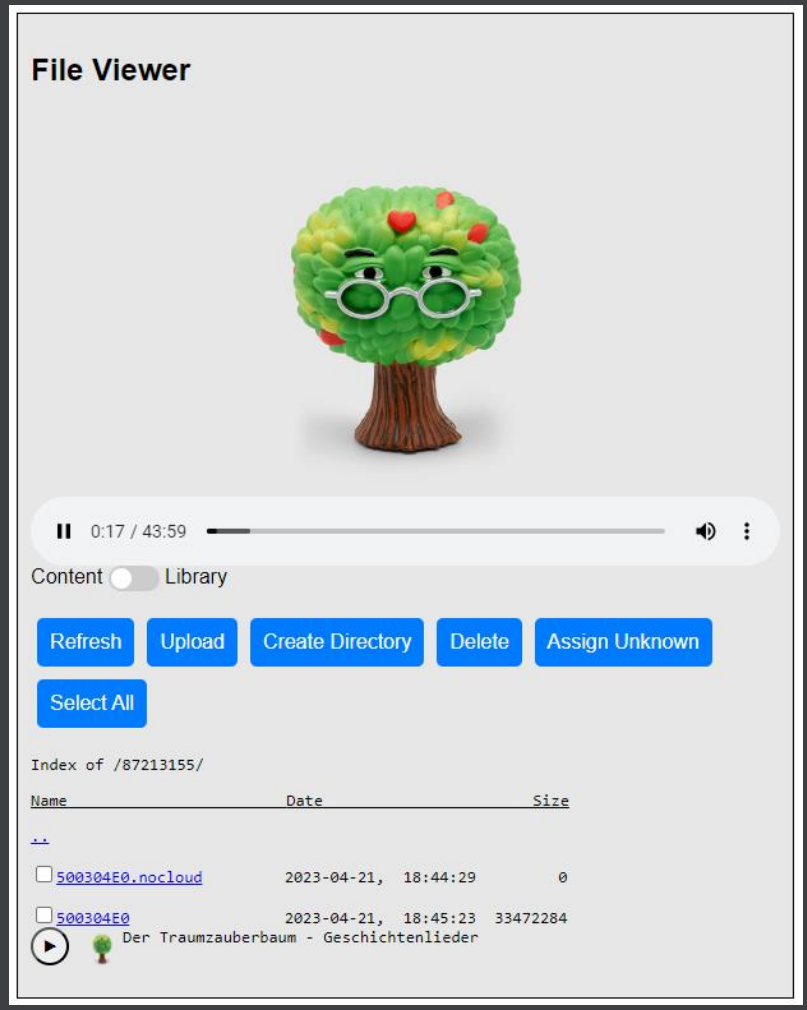
HTTPS

- Client Cert RSA-2048
- CA Cert RSA-4096


8GB
microSD HC
Unlocked
Unlocked
Unlocked
RFID
cloud

TeddyCloud (level: hard)

- written in C, few dependencies, portable (Linux, Windows, Docker)
- Box usable without the cloud
- works for all box variants (replacing certificates)
- own content via TeddyBench or web interface
- download of firmware and original tonies
- ESP32 patch via webinterface



Home Assistant Integration

- by analyzing the debug log sent to manufacturer home assistant integration is possible

Privacy

- sends all user interaction to manufacturer cloud
  - volume changes
  - skipping
  - tonie
  - SSIDs in vicinity
- changed privacy statement that they removed SSID transmission

Custom Firmware Hackiebox

CC3200

- PoC Custom Firmware
- File up-/download (to flash or SD card)
- usable for hardware testing

ESP32

- PoC Custom Firmware (Teddybox)

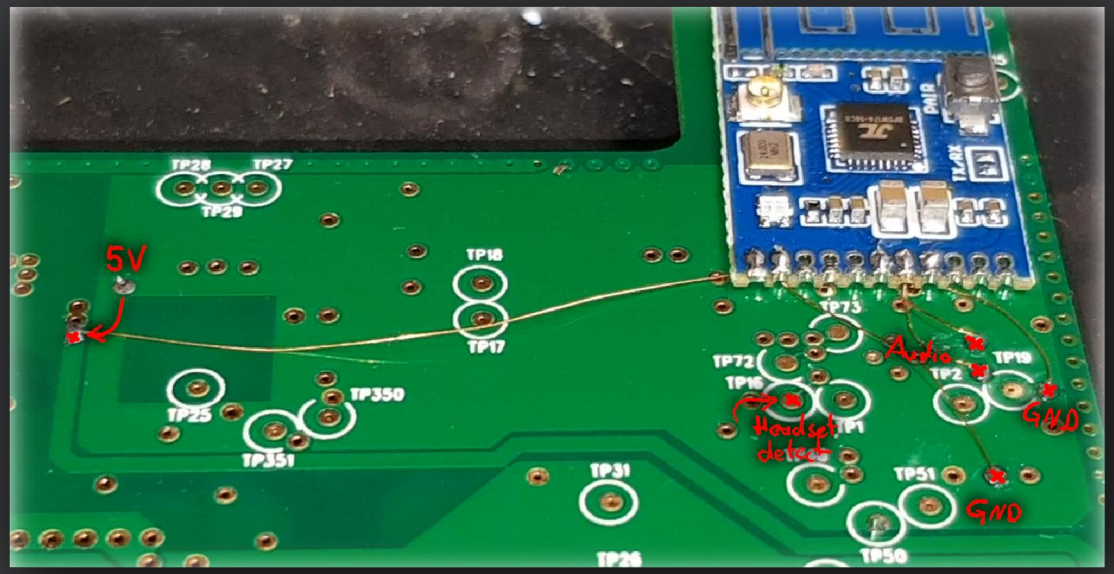
Custom Bootloader HackieboxNG (CC3200)

- two stages
- allows booting the OFW and CFW
- patches OFW on startup
    - disable privacy mode
    - enabling other SLI* tags
    - cloud blocking
    - replacing cloud URLs and CA

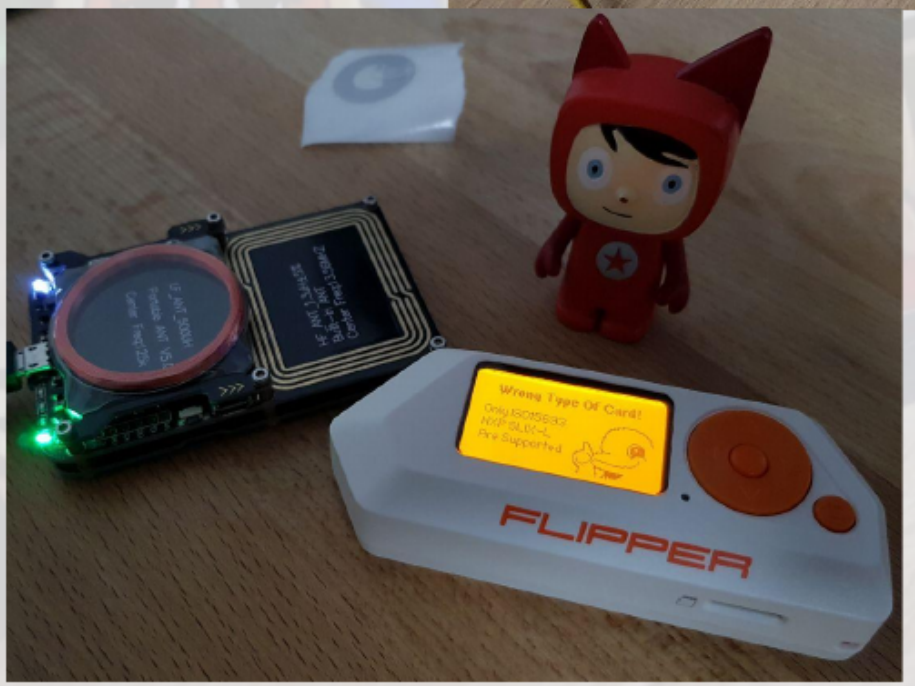
Summary

- decent hardware to play with
- hacker friendly
- own content on the SD card
- prices of used Tonieboxes skyrocketed due to documentation for repairs

Modding


TP28
TP27
TP29
5V
TP18
TP17
TP73
TP72
TP16
Audio
TP2
TP19
GND
Headset detect
TP1
TP350
TP25
TP351
TP31
TP51
GND
TP26
TP50

DIY



Contact us

- GitHub: https://github.com/toniebox-reverse-engineering
- Forum: https://forum.revvox.de/
- Telegram: https://t.me/toniebox_reverse_engineering
- Moritz
  - moritz2342 on Signal
  - @elgolfo@chaos.social on Mastodon

Images

- https://en.wikipedia.org/wiki/Tonies_(company)#/media/File:Toniebox.jpg
- https://www.redbubble.com/i/sticker/I-VOID-WARRANTIES-WITH-PRIDE-LGBTI-by-jillesdotcom/121258026.EJUG5