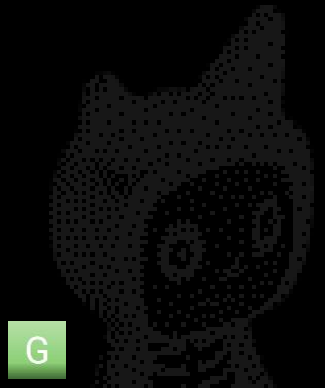
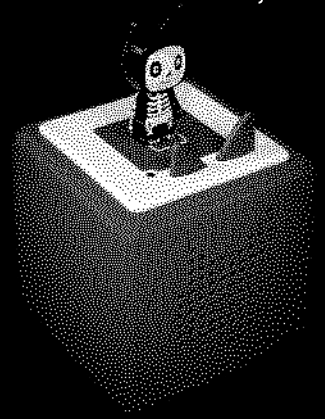
Toniebox Reverse Engineering

Eine Musikbox für Kinder, Maker und Hacker





Ein Team Revvox Projekt

Was ist die Toniebox?

- Lautsprecherbox für Kinder
- NFC-Figuren für Inhalte
- Kein Display
- Schlichtes Design
- Einfache Bedienung

Unsere Motivation

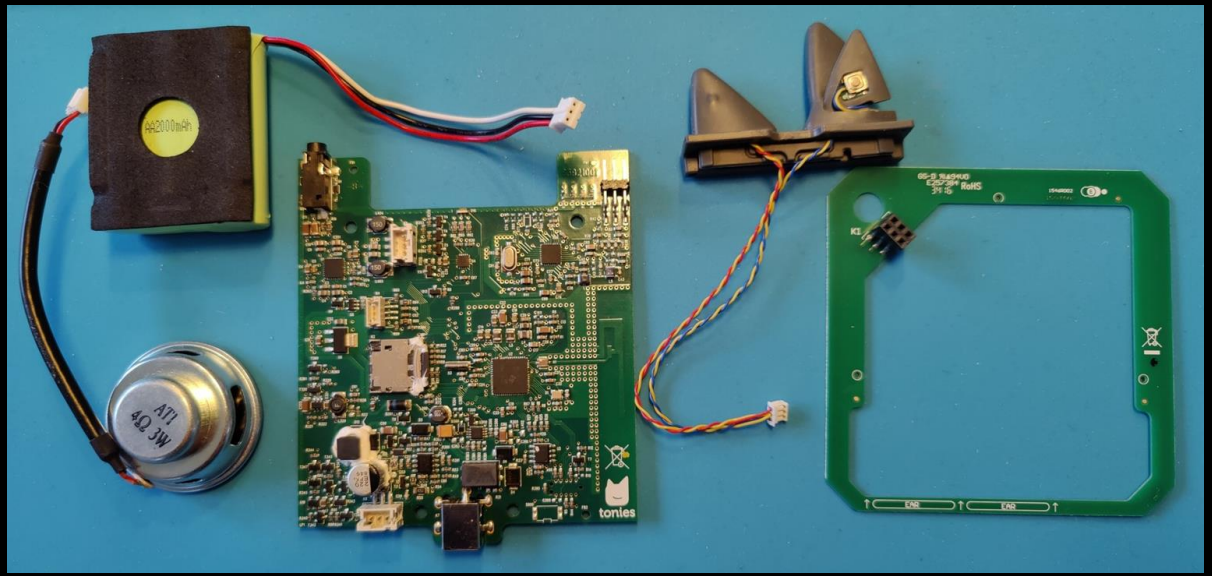
- Ideologische Beweggründe
  - Abhängig von der Cloud eines Herstellers
  - Datenhunger der Hersteller
  - geschlossenes System
- Technische Einschränkungen
  - Nur Originalfiguren, keine eigenen Tags
  - eigene Inhalte nur per Kreativ-Tonie (€€€)
  - künstliches Limit von 90 Minuten

Hardware & Technik

Don't turn it on, TAKE IT APART!

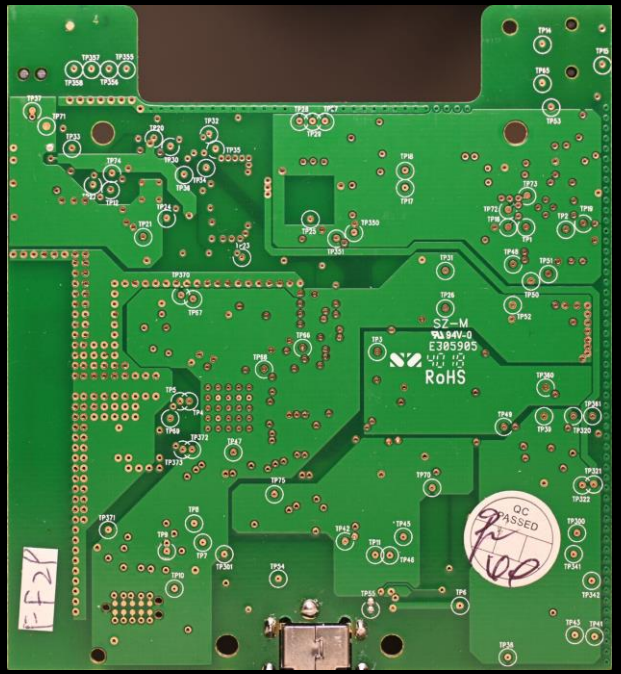
Toniebox von Innen

- Hauptplatine (PCB)
- NiMH-Akku
- Lautsprecher
- Druckknöpfe
- NFC-Antenne



Toniebox PCB

- 4 Layer
- einseitig bestückt
- 82 Testpunkte
- WLAN-Antenne



Toniebox PCB v1/v2

Mikrocontroller (TI CC3200)

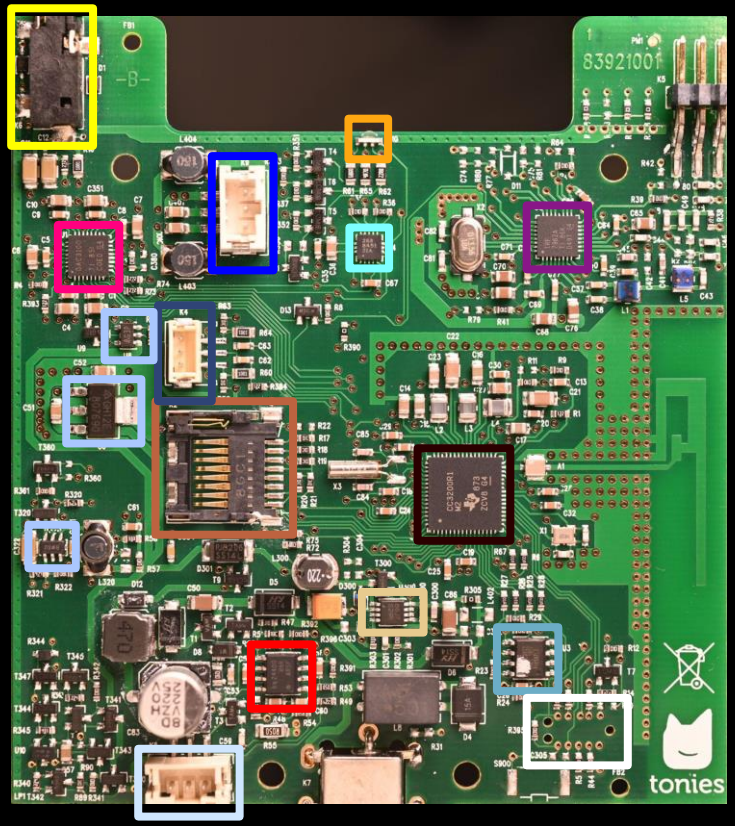
RFID IC (TRF7962A)

MEMS-Accl.sensor (MMA8451QT)

Audio DAC (TLV320DAC3100)

Serial Flash (IS25LQ032B)

SD-Karte



Laderegler (BQ24400)

DC Wandler (LM3485MM)

LDOs/Spannungsversorgung

RGB LED

Audio out

Akku

Ohren

Lautsprecher

Debug IF (Tag Connect)

Toniebox Hardware

- Drei verschiedene µC
  - TI CC3200
  - TI CC3235
  - Espressif ESP32-S3

v1 | v2 | v3 | v4

CC3200 | CC3235 | ESP32-S3

Toniebox CC3200

- Verbreitung: sehr häufig, meist alte Boxen
- Schnittstelle: Tag-Connect
- Flash unverschlüsselt / unsigniert
- cc3200tool zum Lesen / Schreiben über Tag-Connect
- Custom Firmware: Hackiebox
- Custom Bootloader: HackieboxNG

☑ CFW [alpha]

v1 v2

CC3200

Toniebox CC3235

- Verbreitung: selten
- Schnittstelle: Tag-Connect (gesperrt?)
- Zugriff auf Flash über SOP8 Klammer möglich
- Flashinhalt teilweise verschlüsselt
  - Zertifikate unverschlüsselt
  - Firmware signiert und verschlüsselt
- cc3200tool zur Manipulation des Flashdumps

v3

CC3235

Toniebox ESP32

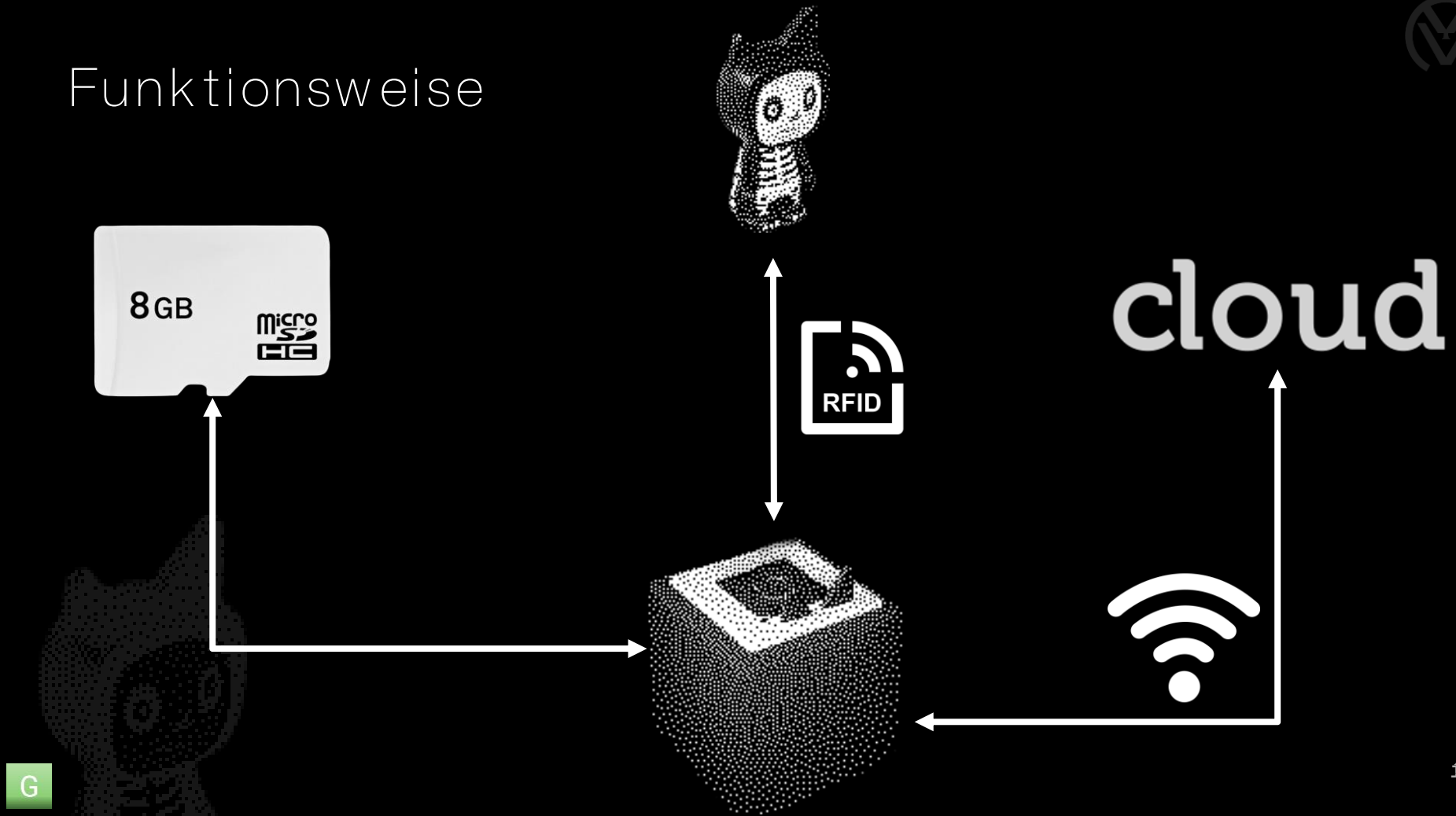
- Verbreitung: im Kommen, neue Boxen
- Schnittstelle: UART (ESP-typisch)
- Zugriff über esptool
- Flash unverschlüsselt / unsigniert
- Custom Firmware
  - Hackiebox PoC ESPuino Port
  - TeddyBox

CFW [alpha]

v4

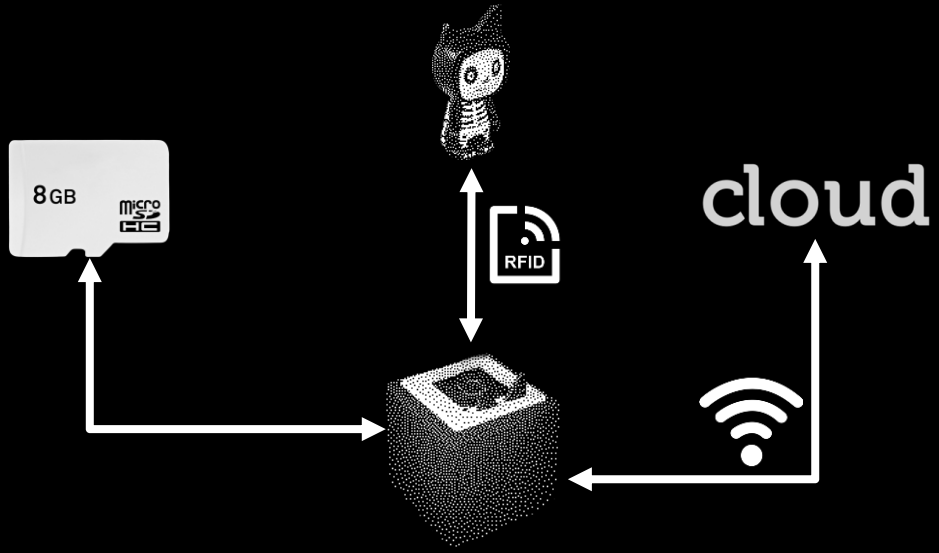
ESP32-S3

Funktionsweise

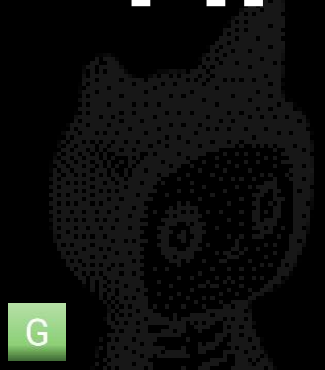


Übertragung der Inhalte

- Stelle Tonie auf
- Lese UID des Tags
- wenn kein Inhalt auf microSD
  - Lese Speicher des Tags
  - Lade Inhalt aus Cloud
  - Schreibe Inhalt auf microSD
- Spiele Inhalt ab



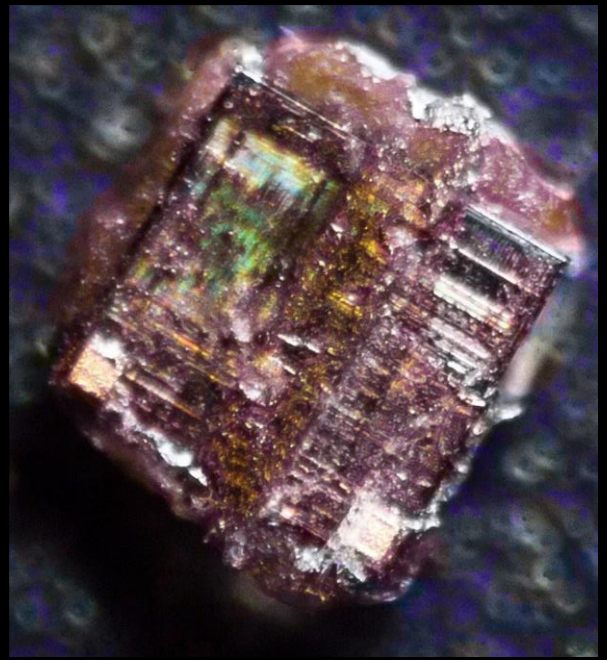
Funktionsweise NFC



...alles muss versteckt sein!

NFC

- Chips: NXP SLIX-L / ISO 15693
- Privacy Mode
- Antenne: Gewickelter Draht
- Fake- / Klon-Tags



NFC

9.4.3.6 ENABLE PRIVACY

Command code = BAh

The ENABLE PRIVACY command enables the ICODE SLIX-L Label IC to be set to Privacy mode if the Privacy password is correct. The ICODE SLIX-L will not respond to any command except GET RANDOM NUMBER and SET PASSWORD.

The XOR password has to be calculated with the password and two times the received random number from the last GET RANDOM NUMBER command:

XOR_Password[31:0] = Password[31:0] XOR {Random_Number[15:0], Random_Number[15:0]}.

To get out of the Privacy status the valid Privacy password has to be transmitted to the IC with the SET PASSWORD command.

Quelle: https://www.nxp.com/products/rfid-nfc/nfc-hf/icode/icode-slix-l:SL2S5002_SL2S5102

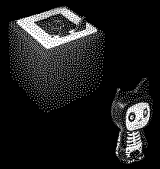
NFC

ISO15693

SLIX-L Custom

Response

Entsperren



GET RANDOM

RAND

SET PASSWORD

:)

Auslesen

INVENTORY

DSFID/UID

READ BLOCK 0-7*

DATA

Sperren

GET RANDOM

RAND

ENABLE PRIVACY

:)

Präsenzdetektion

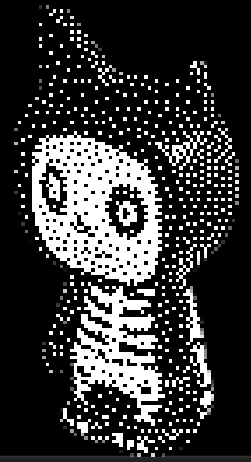
GET RANDOM

RAND

NFC

```
proxmark3> hf 15 cmd sysinfo u
UID:                          E0040350xxxxxxxx
Manufacturer byte: 04, NXP Semiconductors Germany
Chip ID:                      03, IC SL2 ICS50/ICS51(SLI-L)
ICS5002/ICS5102(SLIX-L)
DSFID supported, set to 00
AFI supported, set to 000
Tag provides info on memory layout (vendor dependent)
 4 (or 3) bytes/page x 8 pages
IC reference given: 03

proxmark3> hf 15 dump
Reading memory from tag
UID:                          E0040350xxxxxxxx
Manufacturer byte: 04, NXP Semiconductors Germany
Chip ID:                      03, IC SL2 ICS50/ICS51(SLI-L)
ICS5002/ICS5102(SLIX-L)
Block 00   80 08 D5 12      ....
Block 01   DE D9 F7 6F      ....
Block 02   BA AB 4E 4D      ..N.
Block 03   A1 CE 5C AC      ..\.
Block 04   9E 10 2D 63      .0-.
Block 05   0D F2 41 66      ..A.
Block 06   4F 35 DB 00      O5..
Block 07   8F 25 2F DE      .%/.
```



UUID[8]: E0040350xxxxxxxx

MEM[32]: 8008D512DED9F76F...8F252FDE

SLIX-L Integration

Erweiterung bestehender RFID-Tools

RFID – ISO15693 – SLIX-L

- Proxmark3
  - SLIX-L Unlock fehlt -> implementiert
  - SLIX-L Emulator fehlt -> implementiert

- Flipper Zero
  - SLIX-L Unlock fehlt -> implementiert
  - SLIX-L Emulator fehlt...
    ...ST25R3916 kann keine Emulation...
    ...erlaubt aber pass-thru

RFID - ISO15693 - SLIX-L

A logic 1 starts with an unmodulated time of $256/f_c$ (~18,88 µs) followed by 8 pulses of $f_c/32$ (~423,75 kHz), see Figure 11.

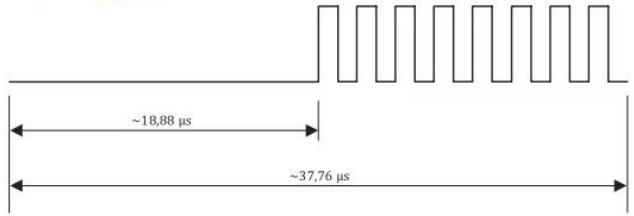
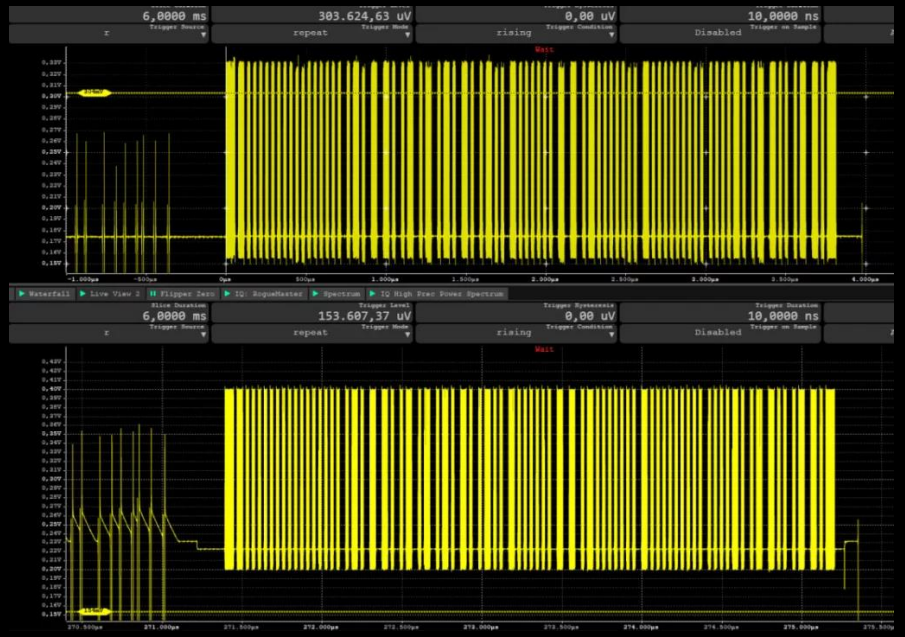


Figure 11 — Logic 1 when using one subcarrier

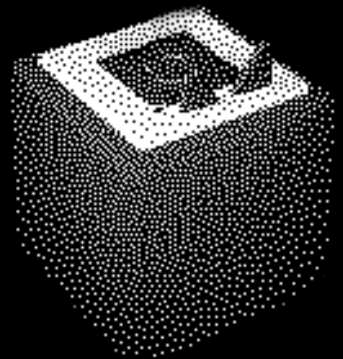


DMA / Timer autoreload

Je übertragenes Bit ~17 Timer-Werte,
bei 32 bit Timer -> ~70 byte je bit,
bei 255 byte payload ~140 KiB RAM-Bedarf

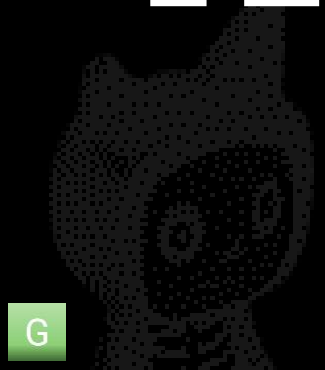

Unlocked


RFID



Funktionsweise SD-Inhalt

einfach nur Protobuf und OPUS



Tonie Audio File (TAF)

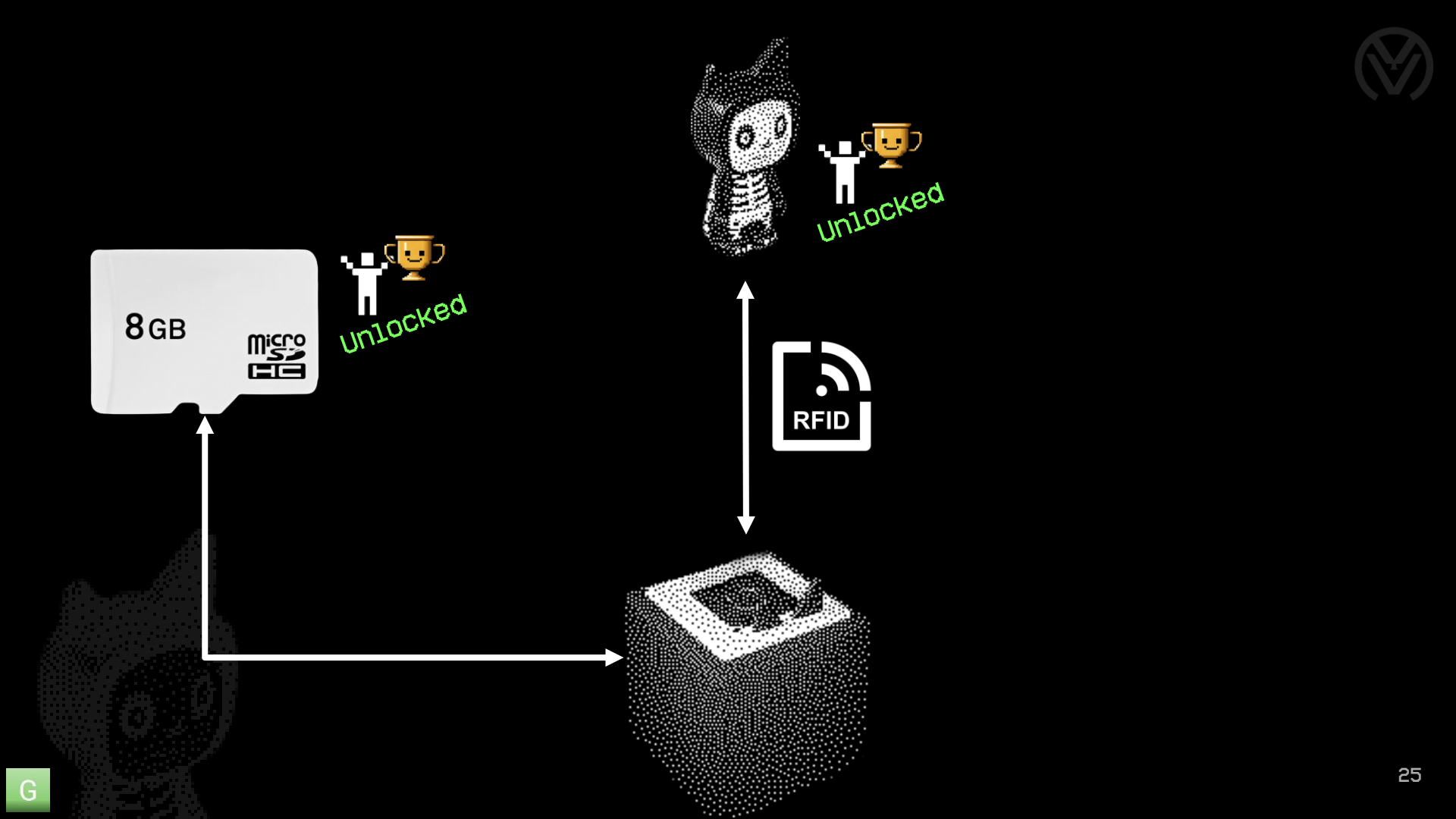
SD:\CONTENT\xxxxxxxx\500304E0

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
	…

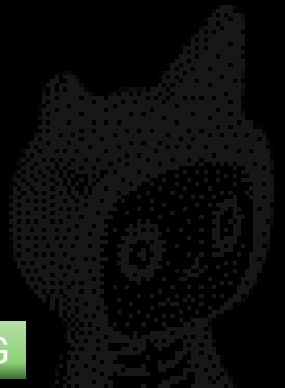
Protobuf coded:
bytes OGG SHA1 hash
uint64_t OGG size
uint32_t OGG audio id
uint32_t[] track / block map
bytes padding

OggS page
OPUS packet
OPUS packet
…
OPUS packet
padding


8GB
micro SD HC
Unlocked
Unlocked
RFID

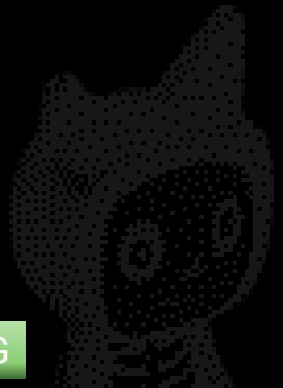
Level Easy TeddyBench

Eine Lösung für jeden Maker



[Video SD entnehmen]

https://www.youtube.com/watch?v=GOZRjaEhrcQ



Tonie-Datenbank – 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-si	
12	01-0010	Conni		
13	01-0011	Conni		
14	01-0012	Bibi Blocksberg	bibi-blo	
15	01-0013	Benjamin Blümchen	benjam	
16	01-0014	Benjamin Blümchen	benjam	
17	01-0018	Kleiner Eisbär		
18	01-0019	Der Grüffelo		
19	01-0020	Die Olchis		
20	01-0021	Unter meinem Bett	unter-m	
21	01-0022	Janosch	janosch	
22	01-0023	Der kleine Drache Kokosnuss	der-klei	
23	01-0024	Bobo Siebenschläfer	bobo-si	
24	01-0025	Teufelskicker	teufelsk	
25	01-0027	Ritter Rost	ritter-ro	

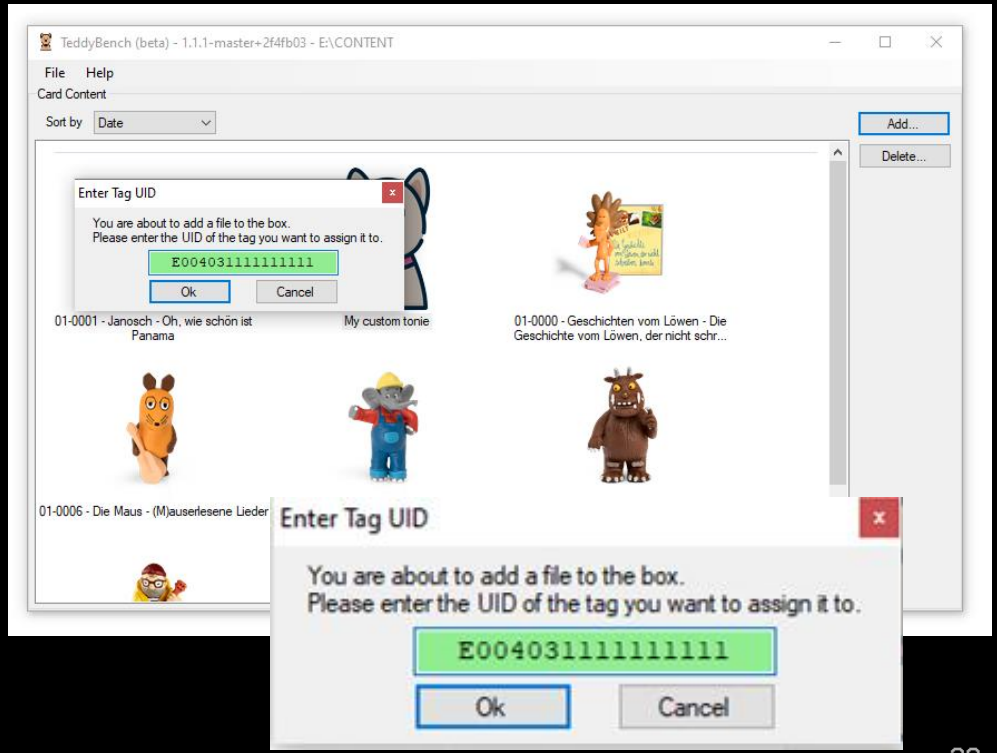

```
{
    "article": "2000001824",
    "data": [
        {
            "series": "Käpt'n Sharky",
            "episode": "Die geheimnisvolle Nebelinsel",
            "release": 1551398400,
            "language": "de-de",
            "category": "audio-play",
            "runtime": 0,
            "age": 4,
            "origin": "tunes",
            "image": "https://cdn.tonies.de/o/images/1_95a23d40b78d9ad5152af5128045bef9395ab72076b5572861a91c46/3_1XCfMnrC1f8RxnpX/kapt_n_sha
            "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)",
```


ca. 1100 Tonies

Quelle: https://github.com/toniebox-reverse-engineering/tonies-json

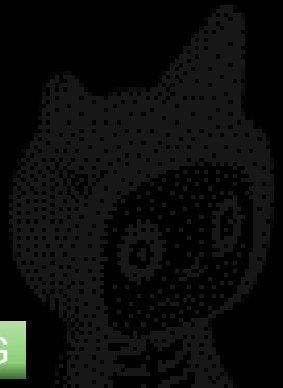
TeddyBench – SD-Management Software

- MP3 → OPUS
- Tonies-Liste
- Nachteile
  - Offline Modus
  - Tags schwer erhältlich
  - Lösung: Patches für die OFW



[Video SD rein]

https://www.youtube.com/watch?v=GOZRjaEhrcQ



G


HAPPY
HAPPY
HAPPY

Funktionsweise Cloud

Wer hat Angst vor(m) MITM?

Cloud-API

HTTPS

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

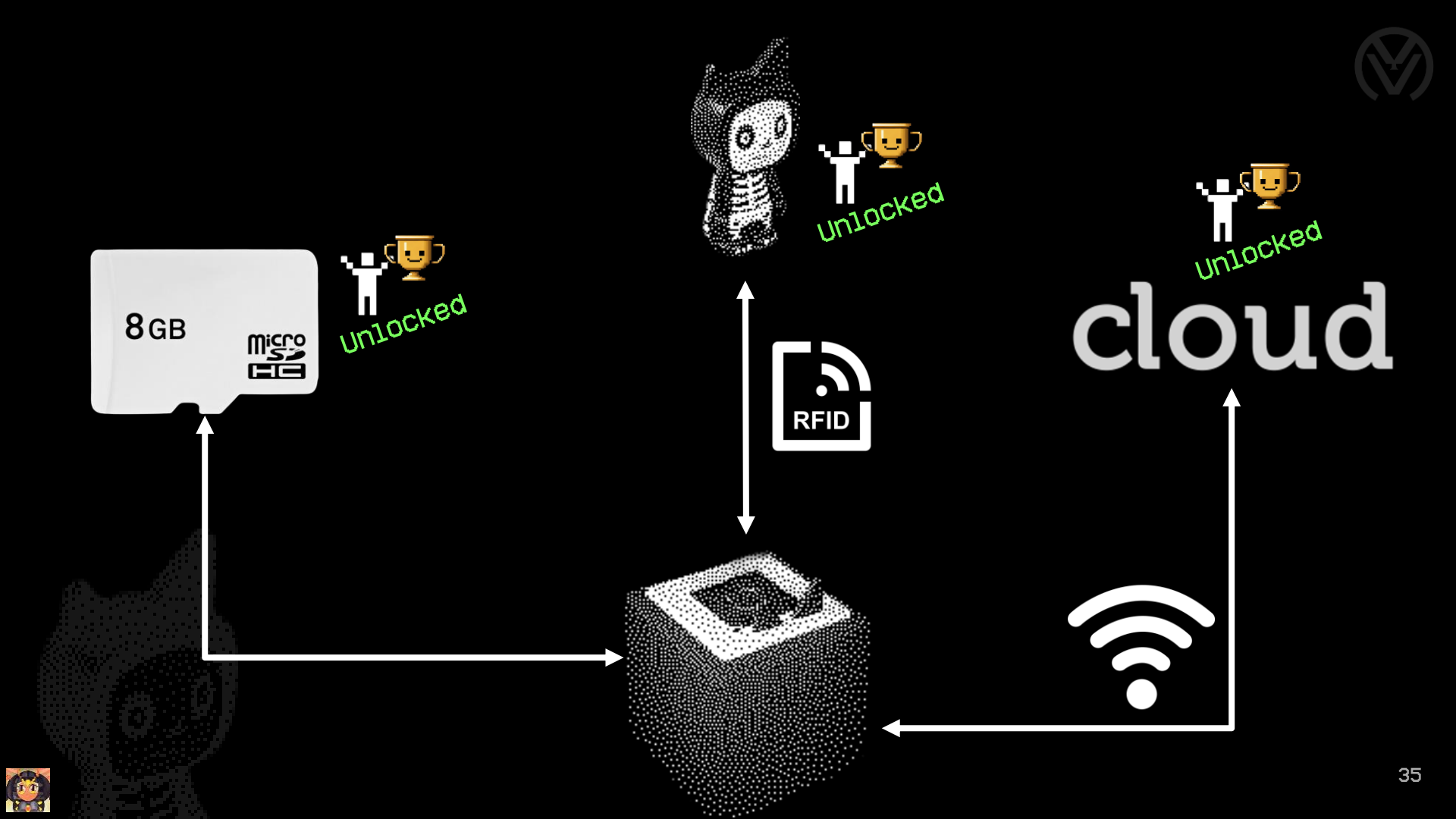
GET

GET+Auth

POST

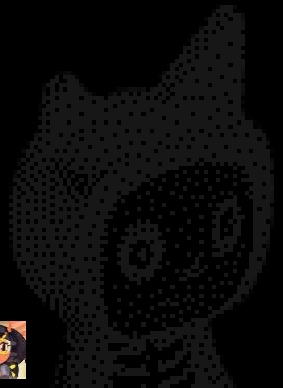
	API	Parameter	Antwort
https://prod.de.tbs.toys/	/v1/time		Unix-Zeit
	/v1/ota	/<file_id>?cv=<time>	Firmware
	/v1/claim	/<UID-rev>	Tonie Audio File
	/v1/content		
	/v2/content		
	/v1/log		
	/v1/cloud-reset		<json>
	/v1/freshness-check	<protobuf>	<protobuf>

https://toniebox-reverse-engineering.github.io/docs/wiki/general/protocol-analysis/


8GB
micro SD HC
Unlocked
Unlocked
Unlocked
RFID
cloud

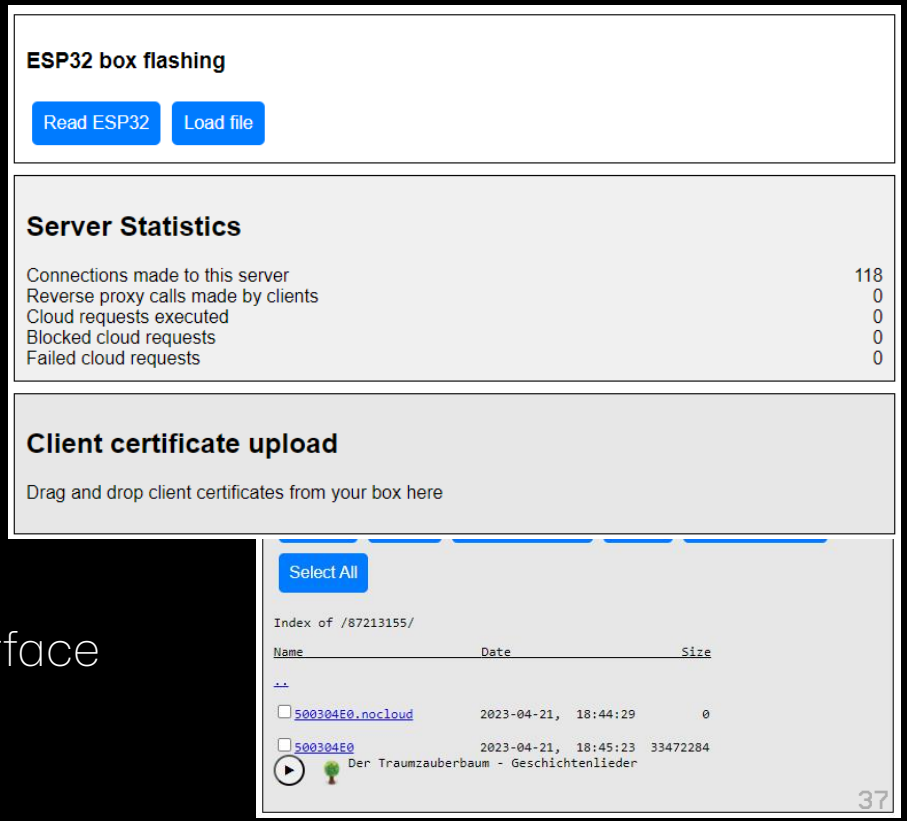
Level Hard TeddyCloud

Etwas C und eine Prise Docker



TeddyCloud – Open Source Cloud Server

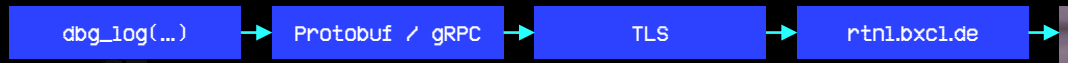
- in C, kaum Abhängigkeiten, portabel
  - Linux, Windows, Docker
- Nutzung der Box ohne Cloud
  - Für alle Chipvarianten (v1-v4)
  - Austausch der Zertifikate
- Eigene Inhalte (TAF)
  - über TeddyBench
  - per Webinterface
- Download von
  - Original-Tonies
  - Firmware
- ESP32 Firmware Patch per Webinterface

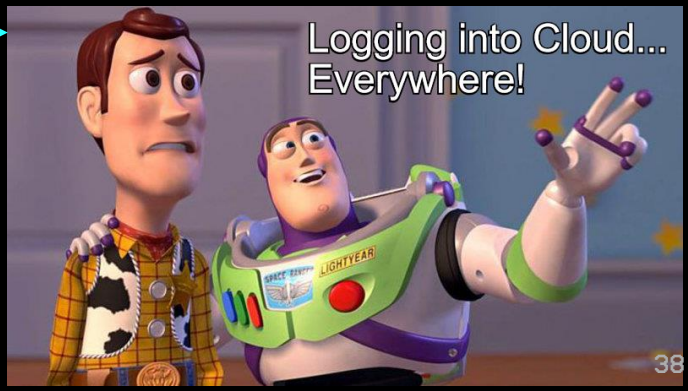


TeddyCloud - Open Source Cloud Server

rtnl.bxcl.de

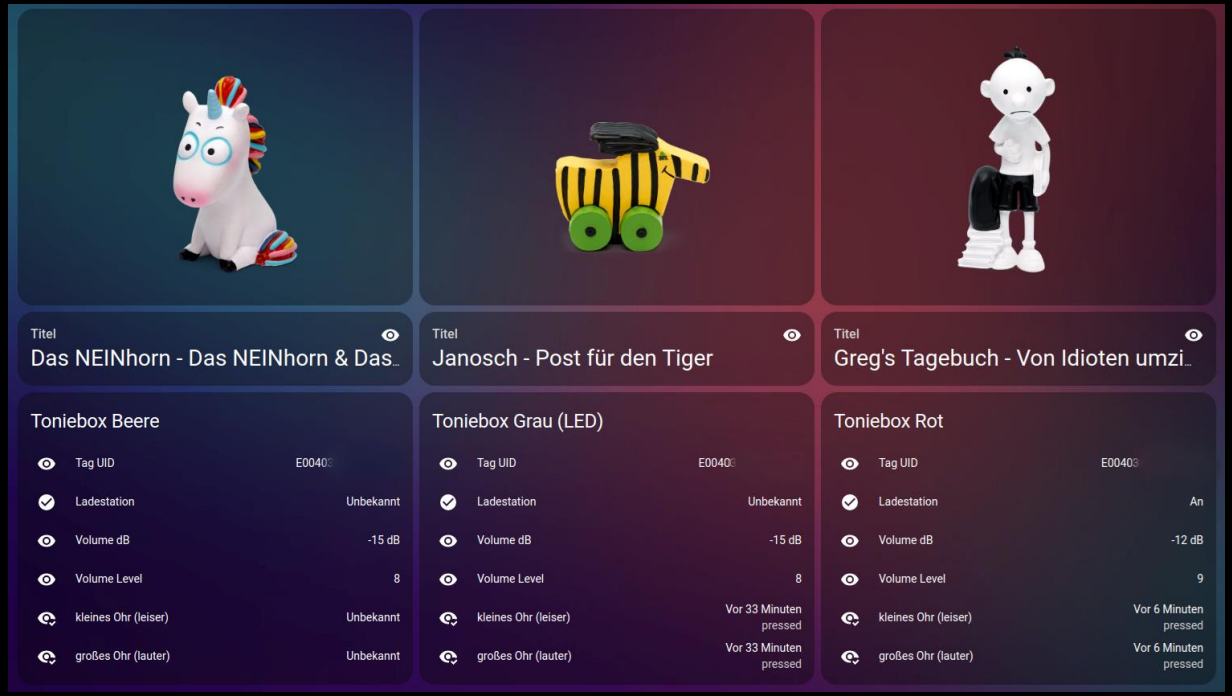
```
1 int dbg_log(unsigned int a1, unsigned int a2, ...)
2 {
3   va_list va; // [sp+28h] [bp-8h]@1
4
5   va_start(va, a2);
6   return rtnl_raw2(a1 >> 16, (unsigned __int16)a1, a2 >> 24, (a2 >> 16) & 0xFF, BYTE1(a2), a2, 0, 0, va);
7 }
```





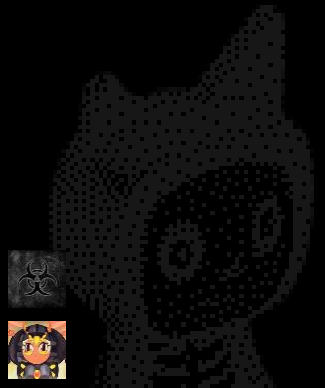
TeddyCloud – Open Source Cloud Server

- Auswertung des RTNL-Datenstroms - MQTT + Home Assistant



[Video HASS]

https://www.youtube.com/watch?v=WqVnnrtgd6k

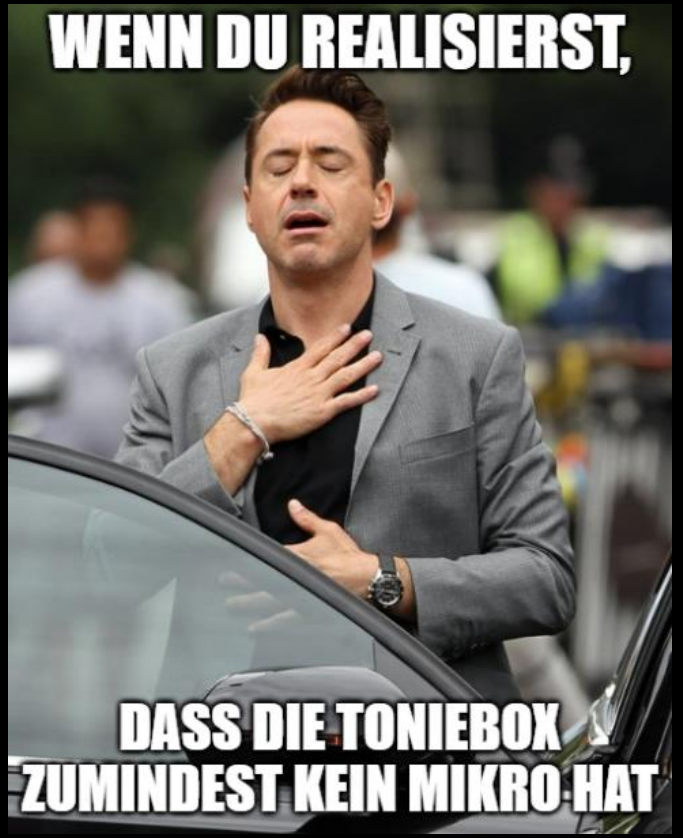


Datenschutz?

"All your data are belong to us"

Toniebox Cloud Kommunikation

- `prod.de.tbs.toys`
  - HTTPS – Tonie Inhalte / Firmware
- `rtnl.bxcl.de`
  - Protobuf / gRPC
  - Logging überall in der Firmware
- Laut Tonies “DSGVO-konform” in Deutschland gehostet (Hetzner)



Datenschutzerklärung

Wenn du deine Toniebox nutzt, versucht sie bei den folgenden Ereignissen eine Verbindung zu mytonies aufzubauen: bei der erstmaligen Inbetriebnahme, beim Anschalten, beim Aufstellen eines ihr unbekannten Tonies, bei einer von dir ausgelösten Suche nach neuen Inhalten. Ist die Verbindung zu mytonies erfolgreich, übermittelt die Toniebox ihr individuelles Client-Zertifikat, ihre IP-Adresse und einen Timestamp. Bei der Nutzung von Tonies und Toniebox erhalten wir auch Daten zu Bedienungs-Events (Tonie aufgestellt oder entfernt inklusive Kennung des Tonies [...], Lautstärke verändert, Spulen und Skippen, Kopfhörer anschließen oder entfernen; Ladestation anschließen oder entfernen) und welcher Inhalt gerade deinem Tonie zugewiesen ist. Bei der Einrichtung der Toniebox sowie dem Hinzufügen eines weiteren WLANs werden zudem die verfügbaren Netzwerke und das verbundene Netzwerk (SSID) übermittelt. Damit möchten wir unseren Service und unser Produkt für dich kontinuierlich verbessern. Die soeben beschriebenen Datentransfers werden von uns dabei grundsätzlich anonym erhoben und in Server-Logfiles gespeichert, damit wir sie bei Bedarf analysieren können. Wenn du mit unserem Kundenservice in Kontakt trittst und im Rahmen einer Support-Anfrage [...] die Toniebox-ID nennst, werden die bis dato anonymen Daten anfragebezogen mit, eventuell von dir genannten, personenbezogenen Daten verknüpft.

Quelle: https://my.tonies.com/legals/privacy-policy

Datenschutzerklärung

Wenn du deine Toniebox nutzt, versucht sie bei den folgenden Ereignissen eine Verbindung zu mytonies aufzubauen: bei der **erstmaligen Inbetriebnahme**, beim **Anschalten**, beim **Aufstellen** eines ihr **unbekannten Tonies**, bei einer von dir ausgelösten Suche nach **neuen Inhalten**. Ist die Verbindung zu mytonies erfolgreich, übermittelt die Toniebox ihr individuelles **Client-Zertifikat**, ihre **IP-Adresse** und einen **Timestamp**. Bei der Nutzung von Tonies und Toniebox erhalten wir auch Daten zu Bedienungs-Events (Tonie aufgestellt oder entfernt inklusive Kennung des Tonies [...], Lautstärke verändert, Spulen und Skippen, Kopfhörer anschließen oder entfernen; Ladestation anschließen oder entfernen) und welcher Inhalt gerade deinem Tonie zugewiesen ist. Bei der Einrichtung der Toniebox sowie dem Hinzufügen eines weiteren WLANs werden zudem die verfügbaren Netzwerke und das verbundene Netzwerk (SSID) übermittelt. Damit möchten wir unseren Service und unser Produkt für dich kontinuierlich verbessern. Die soeben beschriebenen Datentransfers werden von uns dabei grundsätzlich anonym erhoben und in Server-Logfiles gespeichert, damit wir sie bei Bedarf analysieren können. Wenn du mit unserem Kundenservice in Kontakt trittst und im Rahmen einer Support-Anfrage [...] die Toniebox-ID nennst, werden die bis dato anonymen Daten anfragebezogen mit, eventuell von dir genannten, personenbezogenen Daten verknüpft.

Quelle: https://my.tonies.com/legals/privacy-policy

Datenschutzerklärung

Wenn du deine Toniebox nutzt, versucht sie bei den folgenden Ereignissen eine Verbindung zu mytonies aufzubauen: bei der erstmaligen Inbetriebnahme, beim Anschalten, beim Aufstellen eines ihr unbekannten Tonies, bei einer von dir ausgelösten Suche nach neuen Inhalten. Ist die Verbindung zu mytonies erfolgreich, übermittelt die Toniebox ihr individuelles Client-Zertifikat, ihre IP-Adresse und einen Timestamp. Bei der **Nutzung** von Tonies und Toniebox erhalten wir auch Daten zu Bedienungs-Events (**Tonie aufgestellt** oder **entfernt** inklusive **Kennung** des Tonies [...], **Lautstärke** verändert, **Spulen** und **Skippen**, **Kopfhörer** anschließen oder entfernen; **Ladestation** anschließen oder entfernen) und welcher Inhalt gerade deinem Tonie zugewiesen ist. Bei der Einrichtung der Toniebox sowie dem Hinzufügen eines weiteren WLANs werden zudem die verfügbaren Netzwerke und das verbundene Netzwerk (SSID) übermittelt. Damit möchten wir unseren Service und unser Produkt für dich kontinuierlich verbessern. Die soeben beschriebenen Datentransfers werden von uns dabei grundsätzlich anonym erhoben und in Server-Logfiles gespeichert, damit wir sie bei Bedarf analysieren können. Wenn du mit unserem Kundenservice in Kontakt trittst und im Rahmen einer Support-Anfrage [...] die Toniebox-ID nennst, werden die bis dato anonymen Daten anfragebezogen mit, eventuell von dir genannten, personenbezogenen Daten verknüpft.

Quelle: https://my.tonies.com/legals/privacy-policy

Datenschutzerklärung

Wenn du deine Toniebox nutzt, versucht sie bei den folgenden Ereignissen eine Verbindung zu mytonies aufzubauen: bei der erstmaligen Inbetriebnahme, beim Anschalten, beim Aufstellen eines ihr unbekannten Tonies, bei einer von dir ausgelösten Suche nach neuen Inhalten. Ist die Verbindung zu mytonies erfolgreich, übermittelt die Toniebox ihr individuelles Client-Zertifikat, ihre IP-Adresse und einen Timestamp. Bei der Nutzung von Tonies und Toniebox erhalten wir auch Daten zu Bedienungs-Events (Tonie aufgestellt oder entfernt inklusive Kennung des Tonies [...], Lautstärke verändert, Spulen und Skippen, Kopfhörer anschließen oder entfernen; Ladestation anschließen oder entfernen) und welcher Inhalt gerade deinem Tonie zugewiesen ist. Bei der **Einrichtung** der Toniebox sowie dem Hinzufügen eines weiteren WLANs werden zudem die **verfügbaren** Netzwerke und das **verbundene** Netzwerk (**SSID**) übermittelt. Damit möchten wir unseren Service und unser Produkt für dich kontinuierlich verbessern. Die soeben beschriebenen Datentransfers werden von uns dabei grundsätzlich anonym erhoben und in Server-Logfiles gespeichert, damit wir sie bei Bedarf analysieren können. Wenn du mit unserem Kundenservice in Kontakt trittst und im Rahmen einer Support-Anfrage [...] die Toniebox-ID nennst, werden die bis dato anonymen Daten anfragebezogen mit, eventuell von dir genannten, personenbezogenen Daten verknüpft.

Quelle: https://my.tonies.com/legals/privacy-policy

Datenschutzerklärung

Wenn du deine Toniebox nutzt, versucht sie bei den folgenden Ereignissen eine Verbindung zu mytonies aufzubauen: bei der erstmaligen Inbetriebnahme, beim Anschalten, beim Aufstellen eines ihr unbekannten Tonies, bei einer von dir ausgelösten Suche nach neuen Inhalten. Ist die Verbindung zu mytonies erfolgreich, übermittelt die Toniebox ihr individuelles Client-Zertifikat, ihre IP-Adresse und einen Timestamp. Bei der Nutzung von Tonies und Toniebox erhalten wir auch Daten zu Bedienungs-Events (Tonie aufgestellt oder entfernt inklusive Kennung des Tonies [...], Lautstärke verändert, Spulen und Skippen, Kopfhörer anschließen oder entfernen; Ladestation anschließen oder entfernen) und welcher Inhalt gerade deinem Tonie zugewiesen ist. Bei der Einrichtung der Toniebox sowie dem Hinzufügen eines weiteren WLANs werden zudem die verfügbaren Netzwerke und das verbundene Netzwerk (SSID) übermittelt. Damit möchten wir unseren Service und unser Produkt für dich kontinuierlich verbessern. Die soeben beschriebenen Datentransfers werden von uns dabei grundsätzlich **anonym** erhoben und in Server-Logfiles gespeichert, damit wir sie bei Bedarf analysieren können. Wenn du mit unserem Kundenservice in Kontakt trittst und im Rahmen einer Support-Anfrage [...] die **Toniebox-ID** nennst, werden die bis dato anonymen Daten anfragebezogen mit, eventuell von dir genannten, **personenbezogenen Daten verknüpft**.

Quelle: https://my.tonies.com/legals/privacy-policy

Datenschutz

DSGVO-konform

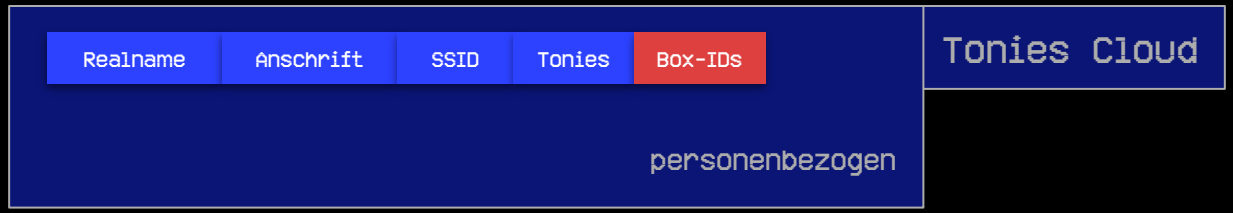
	SSID	Tonies	Box-IDs

personenbezogen

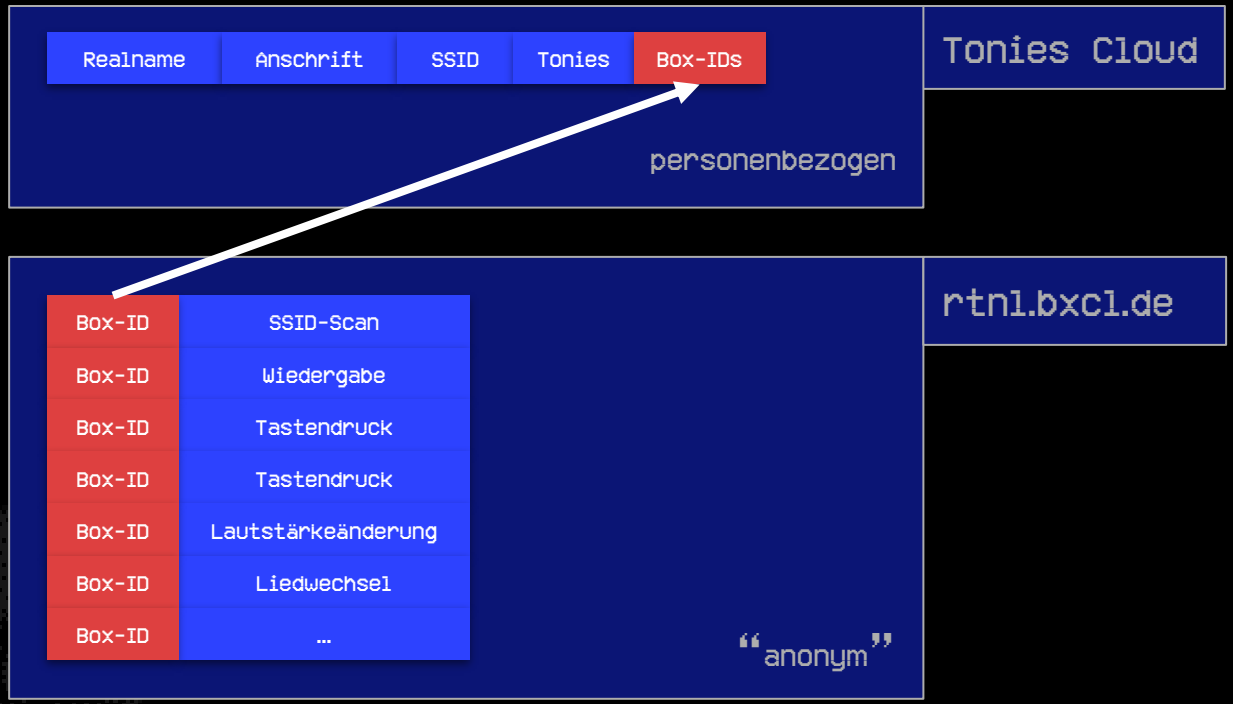
Tonies Cloud

1. **Zu Ihrer Person haben sowie den von Ihnen registrierten Geräten haben, wir folgende Daten gespeichert:**
   - **Vorname:** [redacted]
   - **Nachname:** [redacted]
   - **Postanschrift:** asd1, 12312asdasd
   - **E-Mail-Adresse:** [redacted] (darüber erreichte uns Ihre Anfrage, in der Sie uns Ihre Support-ID mitgeteilt haben, wodurch Sie sich als Eigentümer des Nutzerkontos identifiziert haben, welches mit der E-Mail-Adresse [redacted] registriert ist.
   - **Newsletter-Anmeldung:** Es liegen uns derzeit keine Informationen über eine Newsletter-Anmeldung der o.g. E-Mail-Adressen vor.
   - **Telefonnummer:** 0170[redacted]
   - **Kundennummer:** 569[redacted]
   - **Support-ID:** C[redacted]
   - **Toniebox-IDs:** DJ9-[redacted]; 4KQ-[redacted]
   - **MAC-Adressen:** 0C1[redacted]E0; 3[redacted]7B7
   - **Kreativ-Tonies:** Eine Liste der Kreativ-Tonie-Figuren, die Sie Ihrem Nutzerkonto zugeordnet haben, ist für Sie in Ihrem Kundenkonto über https://my.tonies.com/creative-tonies einsehbar. Wir haben die derzeit Ihrem Konto zugeordneten Kreativ-Tonies nachstehend aufgelistet:
     - [redacted]500E500304E0 (Kreativ-Tonie Spooky),
     - [redacted]E30E500304E0 (Kreativ-Tonie Rot Starterset),
     - [redacted]90F500304E0 (30 Lieblings-Kinderlieder - Spiel- & Bewegungslieder),
     - [redacted]B1B500304E0 (Yoga-Geschichten mit Lama Sara - Mit leichten Übungen zum Entspannen),
     - [redacted]220E500304E0 (30 Lieblings-Kinderlieder - Zählieder)
   - **Audio-Inhalte auf Kreativ-Tonies:** Den Audioinhalt können Sie sich jeweils in Ihrem Nutzerkonto herunterladen, verwalten oder löschen. Wählen Sie dafür über https://my.tonies.com/creative-tonies einen Kreativ-Tonie aus und gelangen so zu den Inhalten.

Datenschutz



Datenschutz



Datenschutz

Wir sind keine Juristen ¯_(ツ)_/¯

SSID-Scan

Moment, da war doch was…

ESP32-Boxen

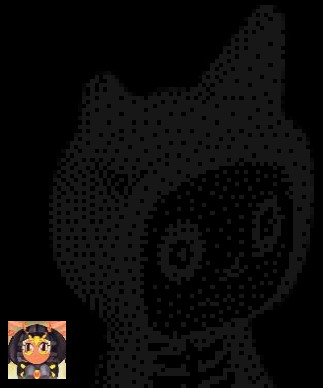
```
esp_wifi_80211_tx()
```

```
char *fake_ssids[] = {
    "01 If you can read this",
    "02   you just violated ",
    "03      my privacy     "
};
```

cloud

```
' ASCII: '....guest.g3gg0.de.........'
..g3gg0.de.........'
00FF000000DDFFFFFF' ASCII: '....01 If you can read this.........'
00FF000000DDFFFFFF' ASCII: '....02   you just violated .........'
00FF000000DDFFFFFF' ASCII: '....03      my privacy     .........'
FFFFFF' ASCII: '....FRITZ!Box 7590 JE.........'
0000AAFFFFFF' ASCII: '....FRITZ!Box Gastzugang.........'
I: '....WLAN-CE57VE.........'
```

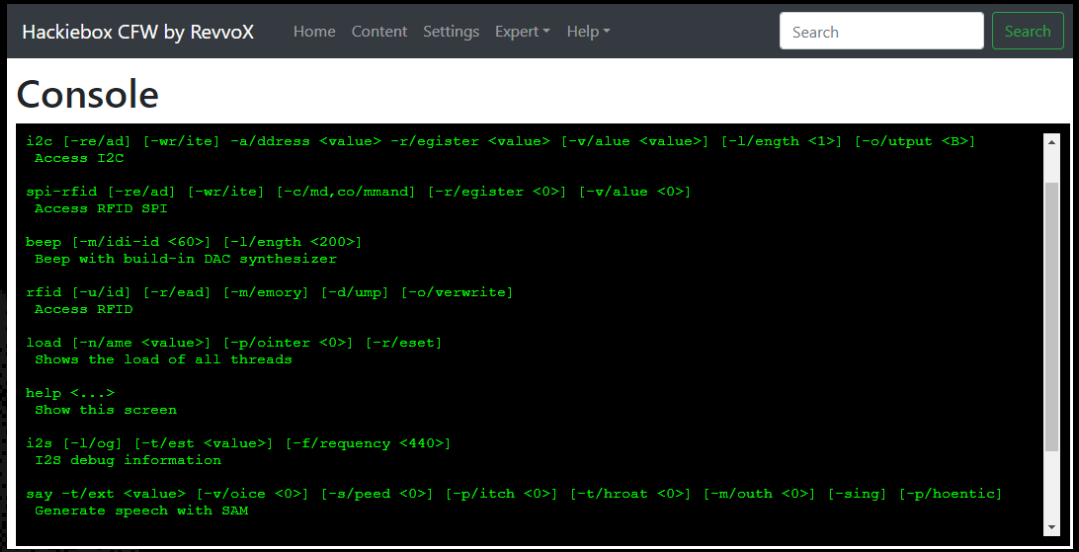
Hackiebox(NG)

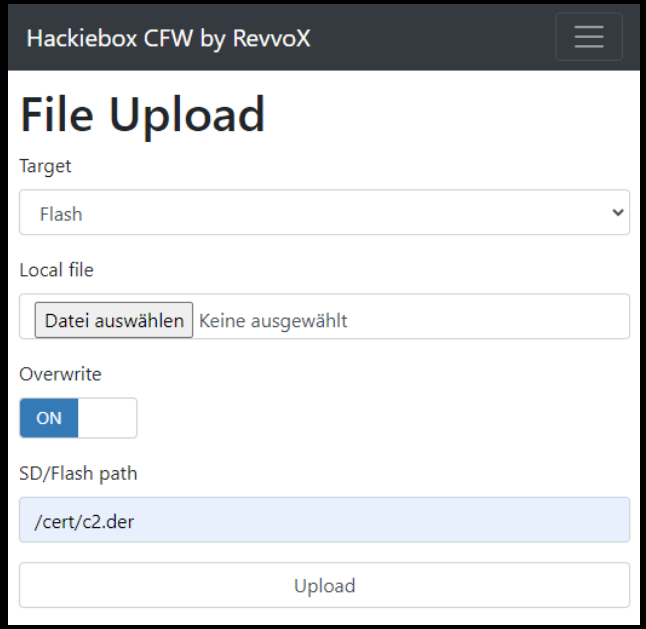


Warum denn keine eigene Firmware?

Custom Firmware Hackiebox (CC3200)

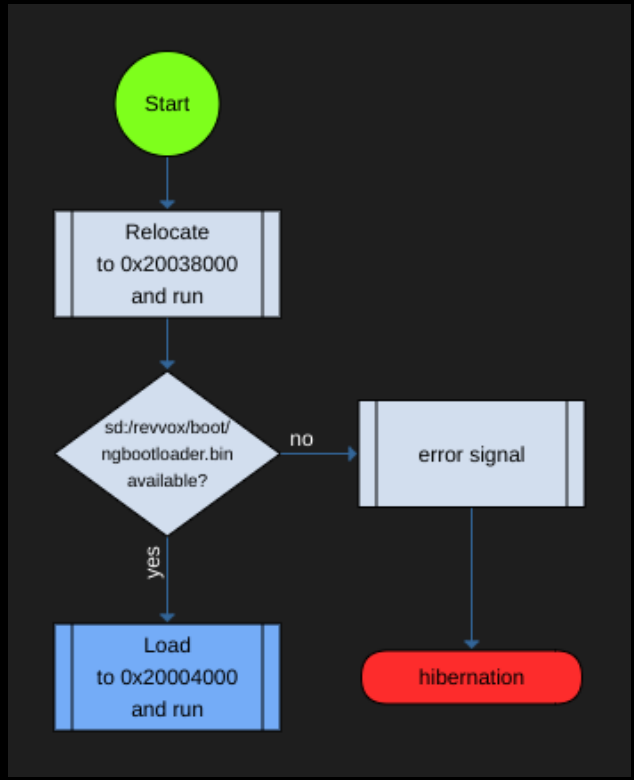
- PoC Custom Firmware
- Datei Up- & Download (Flash/microSD)
- Hardware Test



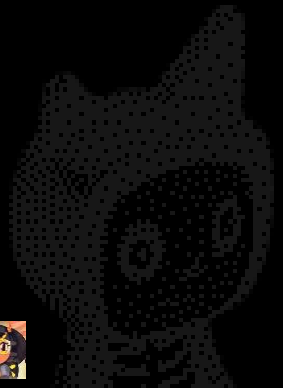


Custom Bootloader Hackiebox NG (CC3200)

- Custom Bootloader
- Zwei Stages
  - Stage 1 - Preloader
  - Stage 2 - Bootloader
- Erlaubt Booten der OFW oder CFW
- Patchen der OFW beim Start
  - Privacy Mode abschalten
  - Freischalten von SLI*-Tags
  - Blockieren der Cloud
  - Ersetzen der URLs der Cloud + CA



Modding

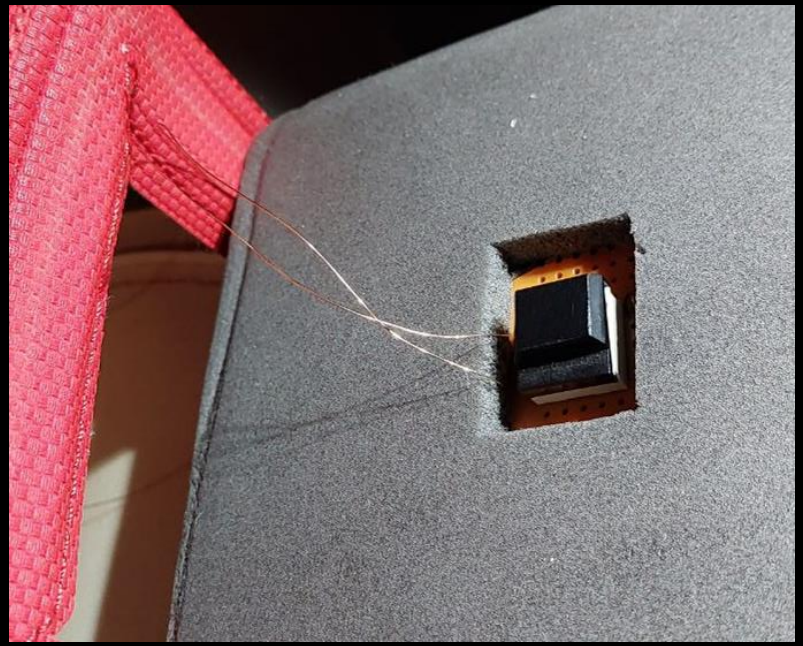


und natürlich auch Reparatur!

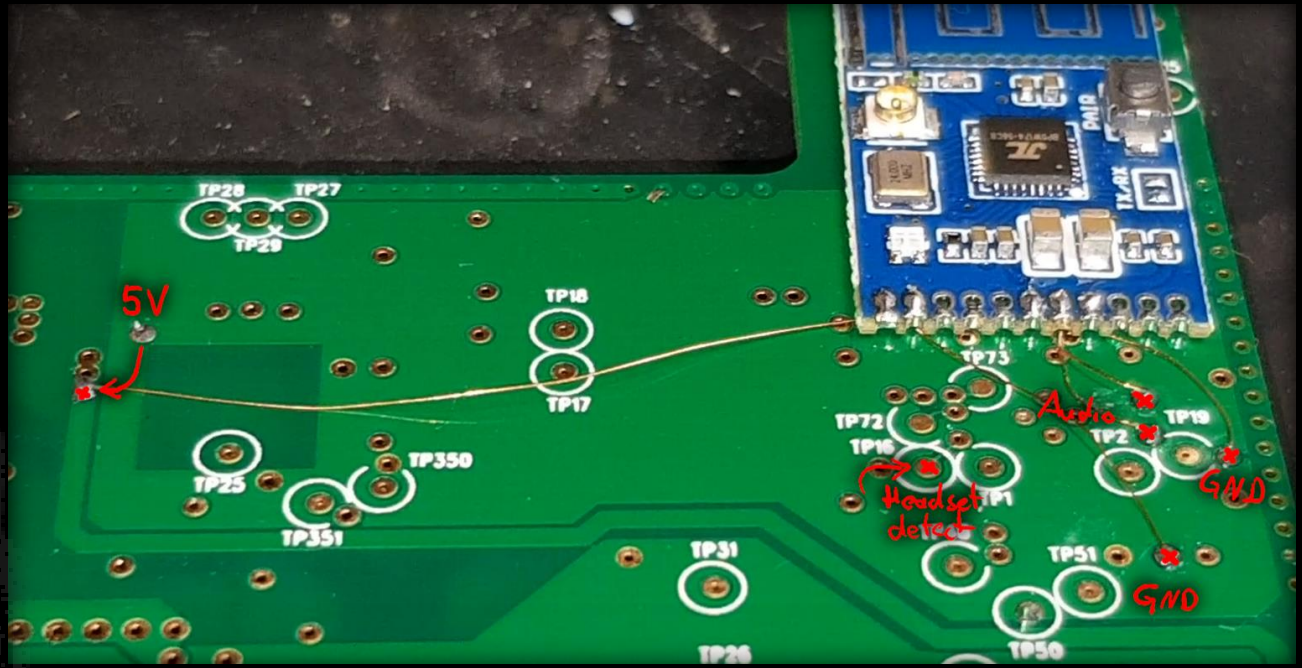
DIY

Beschleunigungssensor-Emulator

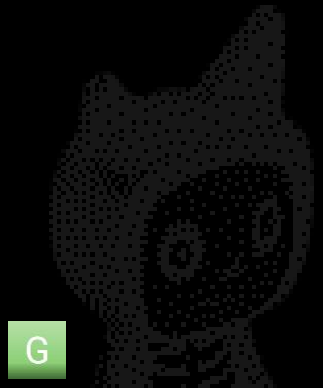
- Emulator für MMA8451Q Beschleunigungssensor
- Raspberry Pi Pico an I2C



Bluetooth Audio Mod



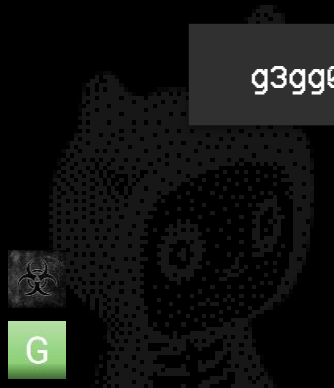
Das Team



Wir sind Team Revvox

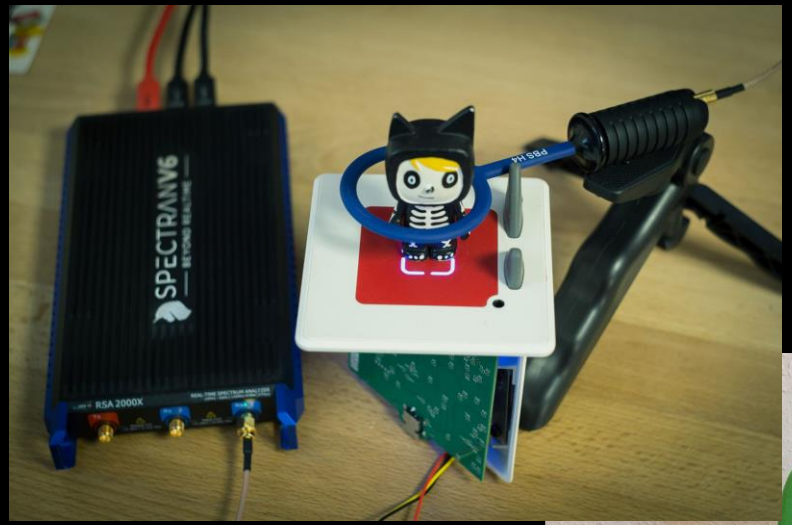
Wer sind wir?

Gambrius	Kommunikation	Datenmanagement	
0xbadbee	Software Rev Eng / Entwicklung	Hardware Rev Eng	Datenmanagement
Moritz	Hardware Rev Eng		
g3gg0	Software Rev Eng / Entwicklung	Hardware Rev Eng	



Danksagung

- bluenazgul
- nv1t
- Aaronia AG
- Lab401
- Telegram RevvoX Community
- Philipp
- RFIDfriend



Kontakt - DECT 8061

0xbadbee

- Vor Ort: Tag 1, 2
- DECT: 8337
- Telegram: @ripitex

g3gg0

- Vor Ort: Tag 1
- DECT: 6360
- Telegram: @g3gg0
- Web: https://g3gg0.de

Gambrius

- Vor Ort: Tag 1
- DECT: 5248
- Telegram: @gambrius
- Web: https://gt-blog.de
- Mail: gambrius@gmail.com

Moritz

- Vor Ort: Tag 1-4
- DECT: 2556
- @elgolfo@chaos.social
- Telegram: @el_golfo
- Web: https://nerdgenieur.me

Kontakt: https://github.com/toniebox-reverse-engineering/talks/blob/37c3-edit/contact.md
GitHub: https://github.com/toniebox-reverse-engineering
Telegram: https://t.me/toniebox_reverse_engineering