

Dissecting the Teddy Ruxpin: Reverse Engineering the Smart Bear

By: @Zenofex

Bio



- @Zenofex
 - Security researcher at Cylance
 - Founding member of Exploitee.rs
 - Contributing member of AustinHackers

Exploitee.rs

AgentHH
CJ_000
Cody

Gynophage
Maximus64
[mbm]

Saurik
Tdweng
x00String

And me!

- We hack things
 - Check out our network of websites for more embedded device research.
 - <https://Exploitee.rs>

Disclaimer

All of the data within this presentation was reverse engineered by reviewing the hardware and software within the Teddy Ruxpin and a lot of trial and error.

The output of these attempts is the content of this presentation and may vary from the manufacturer's documentation.

Terminology



- Illiop – A brown and bear-like creature with a kind disposition.

The OG Illiop



- Released in 1985
- Original used cassette tapes and physical books
- Hardware consisted of
 - Moving eyes
 - Moving Mouth
 - Speaker
- Best selling toy of 1985, 1986

The New Illiop

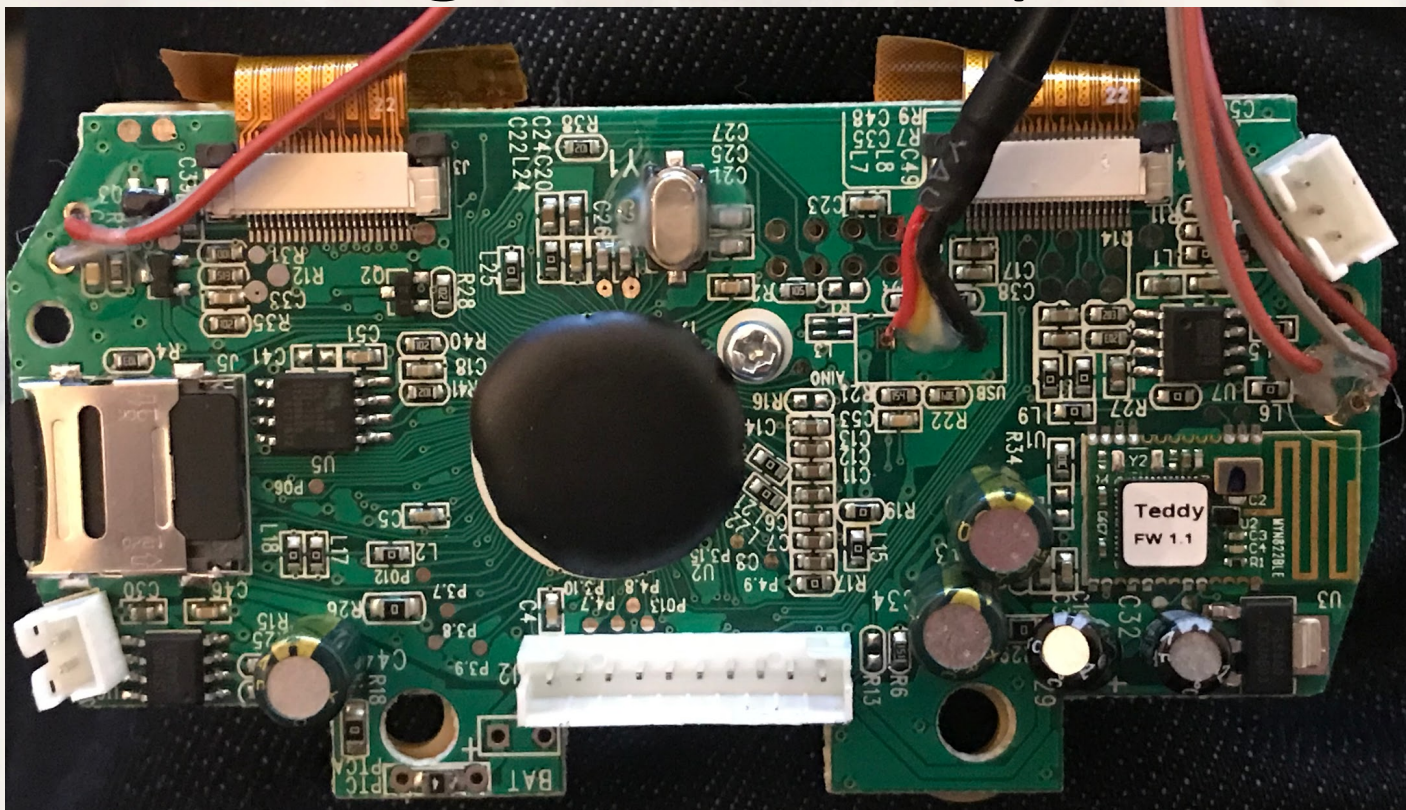


- Animated eyes
- Moving mouth
- Speaker
- BLE
- USB mass storage
 - Pivoted off an internal uSD card
- Companion mobile App

Getting Inside Of Teddy



Logic Board Top



SNC7001A – Sonix MCU

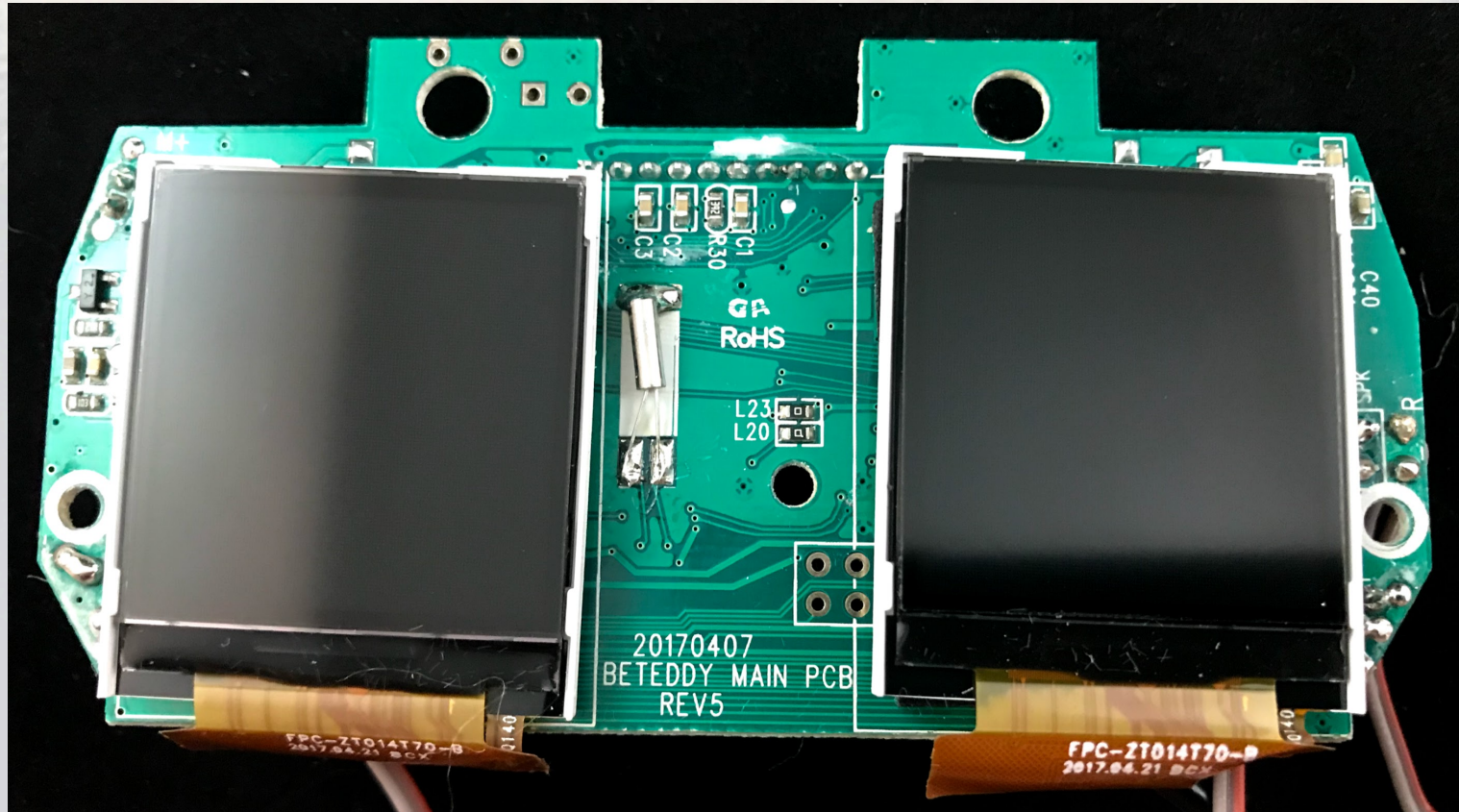
SD-Card slot

SNAP01ASG – Sonix speaker driver

NRF51822 – BLE

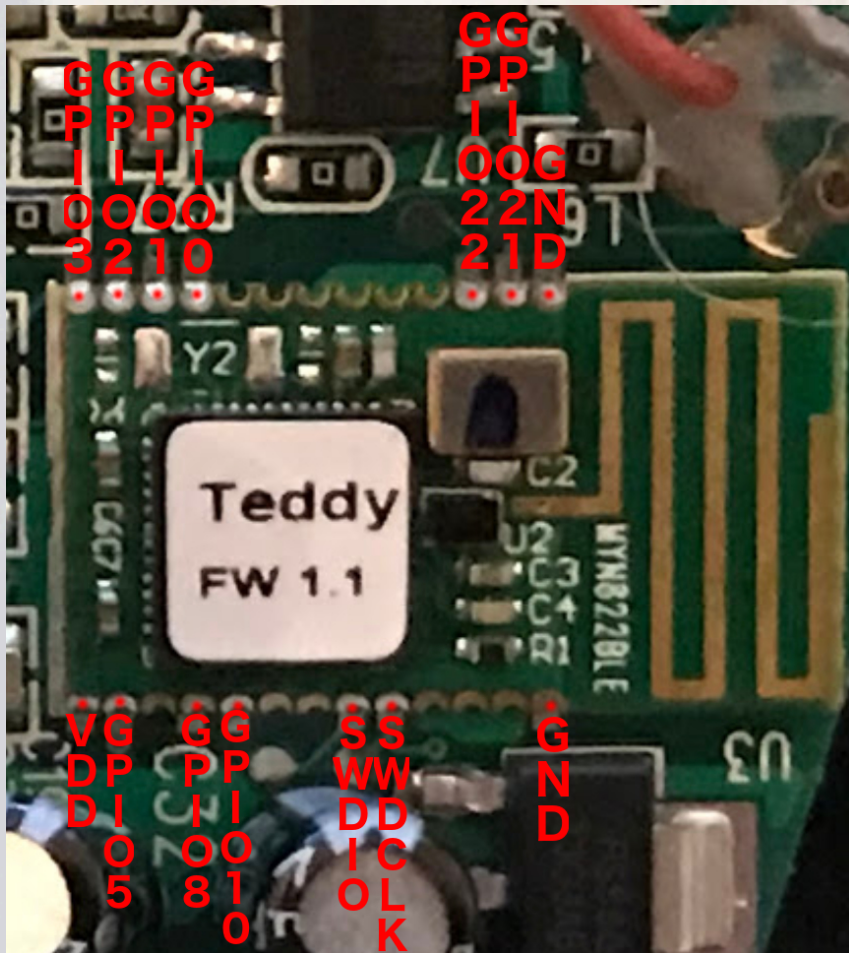
KH25L1606E – SPI flash

Logic Board Bottom



2 x 128 x 128px LCDs

MYN822BLE



nRF51822 based module
– 14 pads connected

- VDD
- 2 x GND
- GPIO 0, 1, 2, 3, 5, 8, 10, 21, 22
- SWDIO
- SWDCLK

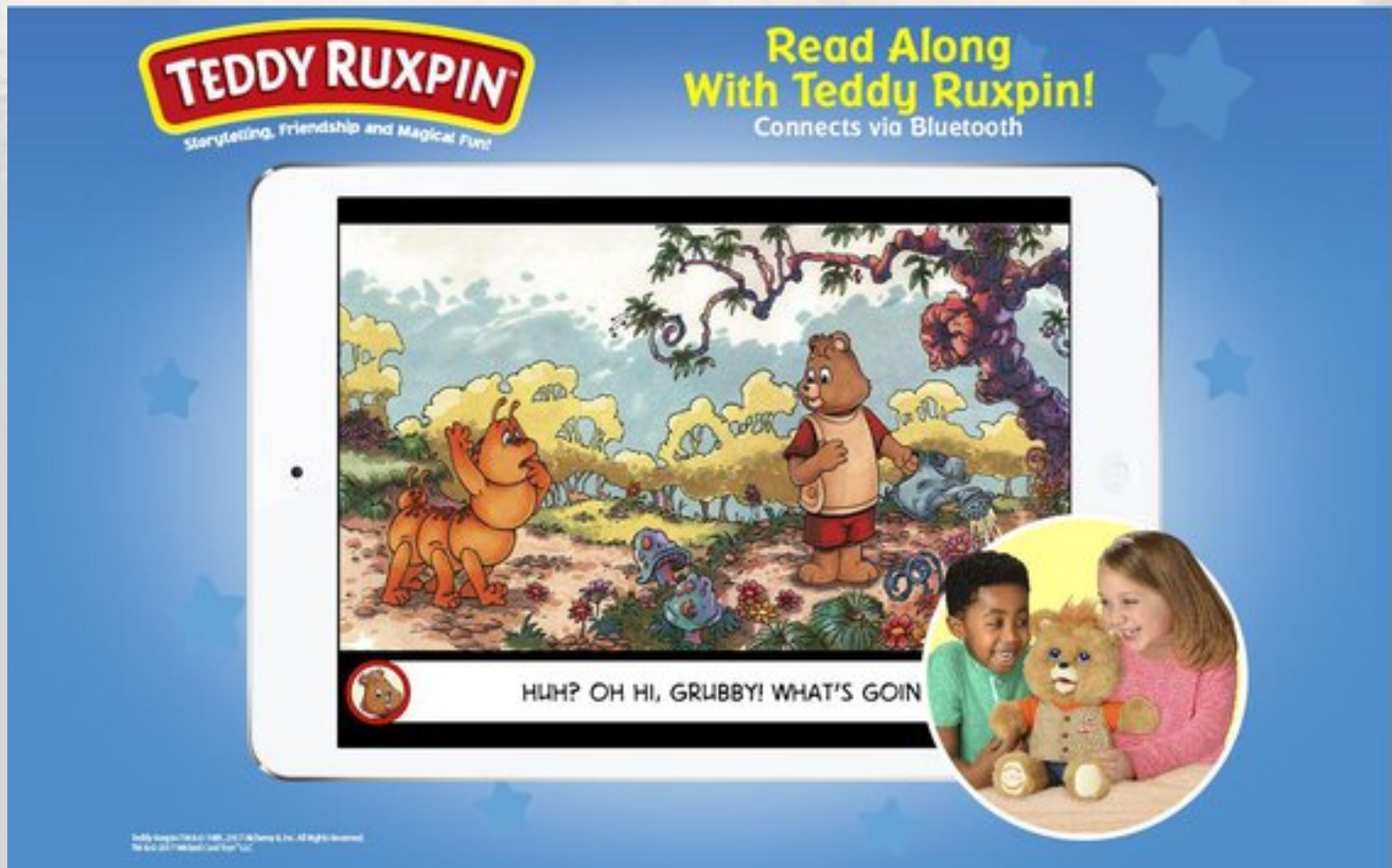
Dumping Firmware w/ SWD

```
0000 0000: C0 07 00 00 D1 06 00 00 D1 00 00 00 B1 06 00 00 .....
0000 0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0000 0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0000 0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0000 0040: EF 00 00 00 F9 00 00 00 03 01 00 00 0D 01 00 00 .....
0000 0050: 17 01 00 00 21 01 00 00 2B 01 00 00 35 01 00 00 .....!+...5...
0000 0060: 3F 01 00 00 49 01 00 00 53 01 00 00 5D 01 00 00 ?...I...S...]...
0000 0070: 67 01 00 00 71 01 00 00 7B 01 00 00 85 01 00 00 g...q...{.....
0000 0080: 8F 01 00 00 99 01 00 00 A3 01 00 00 AD 01 00 00 .....
0000 0090: B7 01 00 00 C1 01 00 00 CB 01 00 00 D5 01 00 00 .....
0000 00A0: DF 01 00 00 E9 01 00 00 F3 01 00 00 FD 01 00 00 .....
0000 00B0: 07 02 00 00 11 02 00 00 1B 02 00 00 25 02 00 00 .....%...
0000 00C0: 1F B5 C0 46 C0 46 00 F0 EF FA 04 B0 0F B4 1F BD ...F.F...
0000 00D0: 08 20 5A 49 09 68 09 58 08 47 38 20 57 49 09 68 .ZI.h.X.G8 WI.h
0000 00E0: 09 58 08 47 3C 20 55 49 09 68 09 58 08 47 40 20 .X.G< UI.h.X.G@
0000 00F0: 52 49 09 68 09 58 08 47 44 20 50 49 09 68 09 58 RI.h.X.G D PI.h.X
0000 0100: 08 47 48 20 4D 49 09 68 09 58 08 47 4C 20 4B 49 .GH MI.h.X.GL KI
0000 0110: 09 68 09 58 08 47 50 20 48 49 09 68 09 58 08 47 .h.X.GP HI.h.X.G
0000 0120: 54 20 46 49 09 68 09 58 08 47 58 20 43 49 09 68 T FI.h.X.GX CI.h
0000 0130: 09 58 08 47 5C 20 41 49 09 68 09 58 08 47 60 20 .X.G\ AI.h.X.G`
0000 0140: 3E 49 09 68 09 58 08 47 64 20 3C 49 09 68 09 58 >I.h.X.G d <I.h.X
0000 0150: 08 47 68 20 39 49 09 68 09 58 08 47 6C 20 37 49 .Gh 9I.h.X.Gl 7I
0000 0160: 09 68 09 58 08 47 70 20 34 49 09 68 09 58 08 47 .h.X.Gp 4I.h.X.G
0000 0170: 74 20 32 49 09 68 09 58 08 47 78 20 2F 49 09 68 t 2I.h.X.Gx /I.h
0000 0180: 09 58 08 47 7C 20 2D 49 09 68 09 58 08 47 80 20 .X.G| -I.h.X.G.
0000 0190: 2A 49 09 68 09 58 08 47 84 20 28 49 09 68 09 58 *I.h.X.G. (I.h.X
0000 01A0: 08 47 88 20 25 49 09 68 09 58 08 47 8C 20 23 49 .G. %I.h.X.G. #I
0000 01B0: 09 68 09 58 08 47 90 20 20 49 09 68 09 58 08 47 .h.X.G. I.h.X.G
0000 01C0: 94 20 1E 49 09 68 09 58 08 47 98 20 1B 49 09 68 .I.h.X.G. I.h
0000 01D0: 09 58 08 47 9C 20 19 49 09 68 09 58 08 47 A0 20 .X.G. I.h.X.G.
0000 01E0: 16 49 09 68 09 58 08 47 A4 20 14 49 09 68 09 58 .I.h.X.G. I.h.X
0000 01F0: 08 47 A8 20 11 49 09 68 09 58 08 47 AC 20 0F 49 .G. I.h.X.G. I
0000 0200: 09 68 09 58 08 47 B0 20 0C 49 09 68 09 58 08 47 .h.X.G. I.h.X.G
0000 0210: B4 20 0A 49 09 68 09 58 08 47 B8 20 07 49 09 68 .I.h.X.G. I.h
0000 0220: 09 58 08 47 BC 20 05 49 09 68 09 58 08 47 00 00 .X.G. I.h.X.G..
0000 0230: 03 48 04 49 02 4A 03 4B 70 47 00 00 00 00 00 20 .H.I.J.K pG....
0000 0240: C0 07 00 00 C0 07 00 00 01 22 D8 4B 5A 60 00 BF .."KZ"...
0000 0250: D7 4A 12 68 00 2A FB D0 01 60 00 BF D4 4A 12 68 .J.h.*...J.h
0000 0260: 00 2A FB D0 00 22 D1 4B 5A 60 00 BF D0 4A 12 68 .*...".K Z"...J.h
0000 0270: 00 2A FB D0 70 47 F0 B5 05 46 0E 46 17 46 00 24 .*.pG...F.F.F.$
0000 0280: 06 E0 A2 00 B1 58 A2 00 50 19 FF F7 DD FF 64 1C ....X...P....d.
0000 0290: BC 42 F6 D3 00 20 F0 BD 01 20 C0 43 C5 49 08 60 .B... ..C.I.`
0000 02A0: 40 10 48 60 70 47 01 46 01 22 92 04 08 68 90 42 @.H`pG.F"...h.B
0000 02B0: 01 D9 10 20 70 47 00 20 FC E7 F0 B5 05 46 0C 46 ...pG....F.F
0000 02C0: 16 46 00 27 06 E0 28 46 21 68 FF F7 BD FF 2D 1D .F.'..(F !h....-
0000 02D0: 24 1D 7F 1C B7 42 F6 D3 F0 BD 70 B5 05 46 0C 46 $....B...p..F.F
0000 02E0: 2E 46 0B E0 30 46 00 F0 75 F9 FF 2C 01 D8 00 24 .F..0F..u....$
0000 02F0: 01 E0 FF 3C 01 3C 01 20 80 02 36 18 00 2C F1 D1 ...<.<...6...
0000 0300: 70 BD 01 46 01 22 12 04 48 68 90 42 01 D9 09 20 p..F."..Hh.B...
0000 0310: 70 47 A9 48 40 69 40 1C 01 D1 0F 20 F8 E7 00 20 pG.H@ie, ...
0000 0320: F6 E7 FE B5 04 46 20 68 03 00 00 F0 37 FA 05 04 .....F h .....7...
0000 0330: 2B 42 49 59 8B 00 20 1D FF F7 E3 FF 05 46 00 2D +BIY... ..F.-
0000 0340: 01 D0 28 46 FE BD FF F7 A7 FF 01 20 C0 02 00 F0 ..(F....
0000 0350: 41 F9 04 22 21 46 99 48 FF F7 8D FF 00 28 01 D0 A..!"F.H .....(
0000 0360: 03 20 EF E7 08 22 21 46 94 48 00 F0 6D F9 00 28 ...."!F.H..m..(
0000 0370: 06 D1 00 21 92 48 00 68 FF F7 66 FF 00 F0 0C F9 ...!H.h..f....
0000 0380: 03 20 DF E7 A7 68 E6 68 60 68 01 90 31 46 38 46 . ...h.h "h..1F8F
```

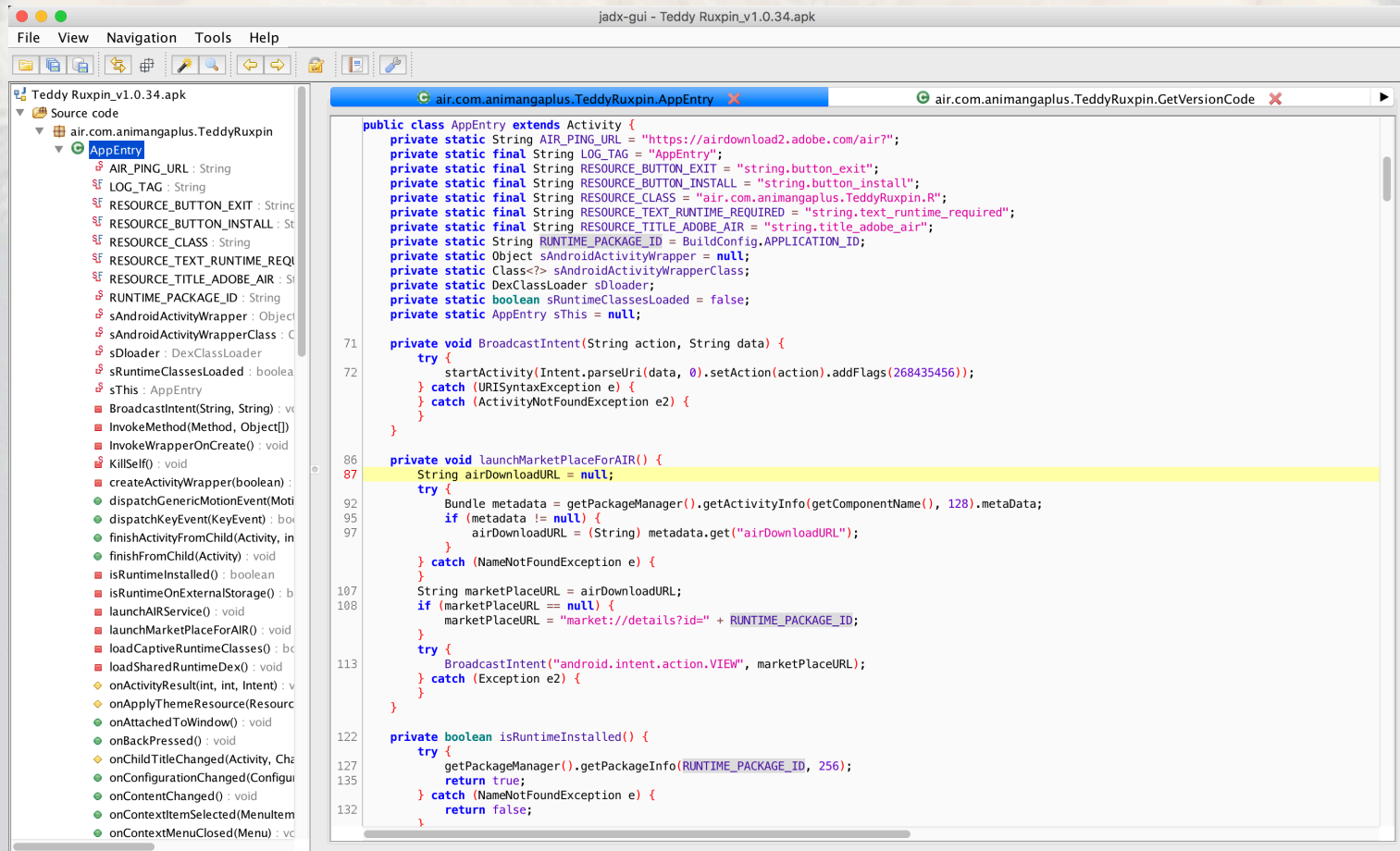
Using MYN822BLE
pin-out and SWD can
dump NRF51822 flash
and RAM

Dump with OpenOCD
or other SWD
compatible utility

Mobile App

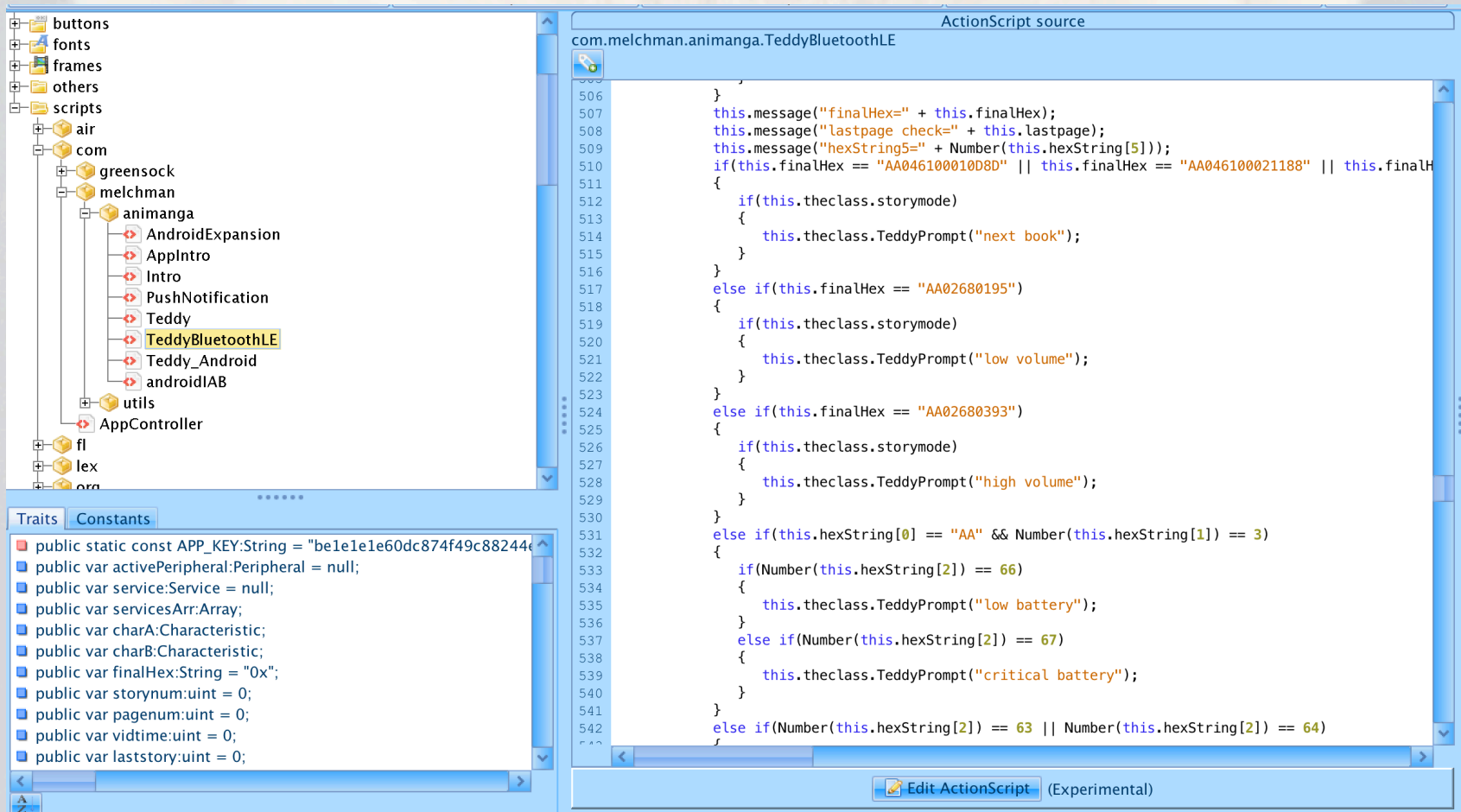


Jadx-GUI



Nothing here, Android app is a wrapper around the Adobe Air content

JPEXS



BLE Info

TX UUID == "a08d0002-ad34-43c8-a046-0744bad310f4"

RX UUID == "a08d0003-ad34-43c8-a046-0744bad310f4"

- Commands
 - AA0403000100F8 – NEXT STORY
 - AA020600F8 – NEXT PAGE
 - AA020500F9 – PAUSE
 - AA020400FA – RESUME
 - AA020100FD – List Books
 - AA020C00F2 – ENTER IN_APP MODE
 - AA020D00F1 – EXIT IN_APP MODE
 - AA021200EC – RESET PURCHASES
- Jump to book commands
 - AA03110001EB
 - AA03110002EA
 - AA03110003E9
 - AA03110004E8
 - AA03110005E7
 - AA03110006E6
 - AA03110007E5
 - AA03110008E4
 - AA03110009E3
 - AA0311000AE2

Firmware

- Firmware dumped with SWD can be examined in IDA
 - Flash Size: 0x20000 (128kb)
 - RAM 0x4000 (16kb)
 - Settings:
 - Create RAM Section
 - RAM Start: 0x20000000
 - Ram Size: 0x4000
 - Load Address: 0x1c000

Teddy Ruxpin Books

- 12 Files
 - Intro.bin
 - Idle.bin
 - 10 x Story##.bin files
- Files are a proprietary package called “SNXROM”
- Target exclusive edition contains 2 extra stories.

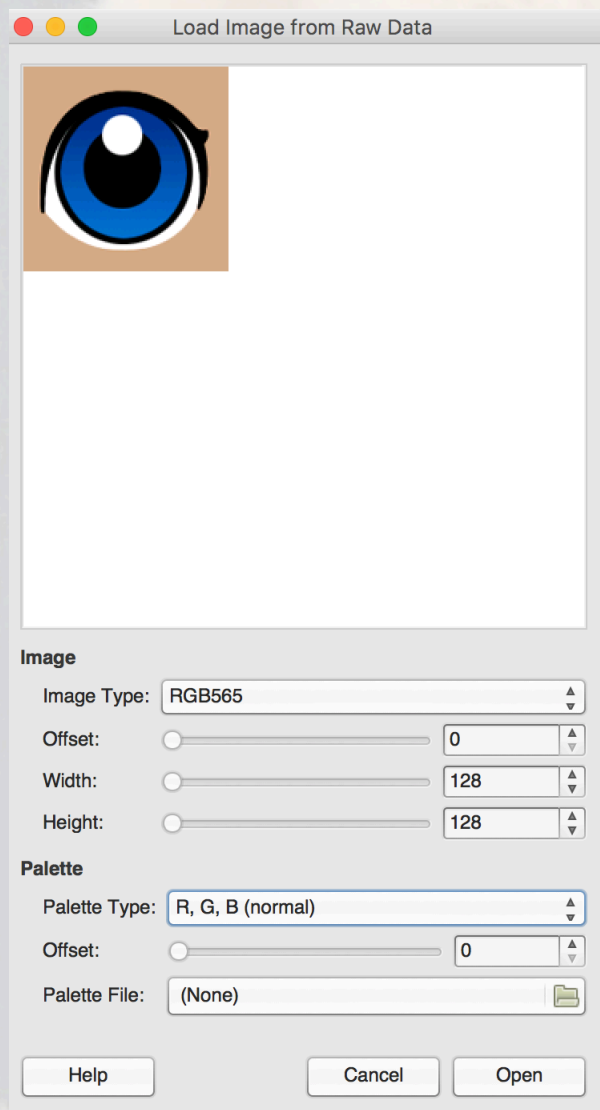
SNXROM

```
Intro.bin
0000 0000: 53 00 4E 00 58 00 52 00 4F 00 4D 00 FF FF FF FF S.N.X.R. 0.M....
0000 0010: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....L...
0000 0020: FF FF FF FF FF FF FF FF 00 04 00 00 4C 00 00 00 .....
0000 0030: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0040: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0050: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0060: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0070: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0080: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0090: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 00A0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 00B0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 00C0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 00D0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 00E0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 00F0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0100: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0110: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0120: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0130: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0140: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0150: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0160: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0170: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0180: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0190: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 01A0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 01B0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 01C0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 01D0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 01E0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 01F0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0200: 00 04 00 00 00 84 00 00 00 04 01 00 00 84 01 00 .....
0000 0210: 00 04 02 00 00 84 02 00 00 04 03 00 00 84 03 00 .....
0000 0220: 00 04 04 00 00 84 04 00 00 04 05 00 00 84 05 00 .....
0000 0230: 00 04 06 00 00 84 06 00 00 04 07 00 00 84 07 00 .....
0000 0240: 00 04 08 00 00 84 08 00 00 04 09 00 00 84 09 00 .....
0000 0250: 00 04 0A 00 00 84 0A 00 00 04 0B 00 00 84 0B 00 .....
0000 0260: 00 04 0C 00 00 84 0C 00 00 04 0D 00 00 84 0D 00 .....
0000 0270: 00 04 0E 00 00 84 0E 00 00 04 0F 00 00 84 0F 00 .....
0000 0280: 00 04 10 00 00 84 10 00 00 04 11 00 00 84 11 00 .....
0000 0290: 00 04 12 00 00 84 12 00 00 04 13 00 00 84 13 00 .....
0000 02A0: 00 04 14 00 00 84 14 00 00 04 15 00 00 84 15 00 .....
0000 02B0: 00 04 16 00 00 84 16 00 00 04 17 00 00 84 17 00 .....
0000 02C0: 00 04 18 00 00 84 18 00 00 04 19 00 00 84 19 00 .....
0000 02D0: 00 04 1A 00 00 84 1A 00 00 04 1B 00 00 84 1B 00 .....
0000 02E0: 00 04 1C 00 00 84 1C 00 00 04 1D 00 00 84 1D 00 .....
0000 02F0: 00 04 1E 00 00 84 1E 00 00 04 1F 00 00 84 1F 00 .....
0000 0300: 00 04 20 00 00 84 20 00 00 04 21 00 00 84 21 00 .....
0000 0310: 00 04 22 00 00 84 22 00 00 04 23 00 00 84 23 00 .....
0000 0320: 00 04 24 00 00 84 24 00 00 04 25 00 00 84 25 00 .....
0000 0330: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0340: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0350: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0360: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0370: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....
0000 0380: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....

Arrow keys move  F find      RET next difference  ESC quit
C ASCII/EBCDIC  E edit file  G goto position  Q quit
```

- Files consist of
 - SNXROM wide char magic string
 - Header
 - Record start
 - Record end
 - Table ends with 0xFFFF
 - Record Data
 - Raw image data is stored first
 - Audio starts with AU

Video Frames



- Video is 128x128 RGB565 frames
- Frame record count is then split between left and right eyes
- Gimp raw data import works great for finding images in blobs of data

Audio32

- Sonix proprietary file format used for audio data and mouth/eye synchronization on the Teddy Ruxpin
- Consists of:
 - Mark table
 - Silence table
 - Audio data
 - Single channel audio

AU32 Header Structure

- Header
 - “AU” (2 bytes)
 - Unknown constant value (2 bytes)
 - Sample rate (2 bytes)
 - Channels (always 1) (2 bytes)
 - Unknown value (4 bytes)
 - Unknown value (4 bytes)
 - Enable mark table
 - Enable silence table
 - Unknown value (4 bytes)
 - Mark table data
 - Silence table data
 - Audio data

Au32 Data Structure

- After the header
 - Mark Table
 - Position (2-4 bytes)
 - If the first bytes are 0x8000 a second value is read and appended to the first bytes
 - Value (2 bytes)
 - Silence Table
 - 0x0 in all TR audio files
 - Audio Data
 - 16 bit signed little endian

Mark Table

- The mark table is used to create synchronized mouth movements within the audio and video frames
- Different mark labels are used to signify how much TR's mouth should move or what image to display
 - 0 – Closed
 - 1 – Half open
 - 2 – Full open
- Anything with higher value is used to reference video frames

Silence Table

- Silence table is used to compress audio by removing empty sections then referencing position and length in table
- Silence table has been unused in all tested TR files

Audio Data

```
0000 0000: 41 55 80 3E 80 0C 01 00 AD 07 00 00 08 33 01 00 AU.>.... 3..
0000 0010: 01 00 00 00 00 00 FF FF 00 00 07 01 FF FF FF FF ..D#.m.
0000 0020: F7 00 44 23 02 00 6D 01 00 00 D5 00 01 00 11 01 ..0.....
0000 0030: 00 00 4F 01 02 00 11 01 00 00 D5 00 01 00 12 01 ..y.....
0000 0040: 00 00 79 00 01 00 B7 00 02 00 11 01 01 00 D5 00 ..[.j...z.
0000 0050: 02 00 F3 00 00 00 83 04 02 00 F4 00 00 00 B6 00 .....j.
0000 0060: 01 00 D5 00 02 00 5B 00 01 00 6A 00 02 00 7A 00 .....j.
0000 0070: 00 00 C6 00 01 00 6A 00 00 00 4C 00 02 00 6A 00 ..=...[.
0000 0080: 01 00 3D 00 02 00 5B 00 00 00 7A 00 00 00 B6 00 ..!.....s.
0000 0090: 02 00 21 01 00 00 D5 00 02 00 02 01 00 00 73 10 .....[.
0000 00A0: 02 00 D4 00 00 00 98 00 02 00 98 00 00 00 98 00 .....s..b.
0000 00B0: 02 00 B7 00 00 00 98 00 01 00 3D 00 02 00 88 00 .....[.
0000 00C0: 00 00 C6 00 02 00 A7 00 00 00 5B 00 02 00 12 01 .....=.
0000 00D0: 00 00 38 01 01 00 3D 00 00 00 AE 00 01 00 4D 00 ..8...=.
0000 00E0: 00 00 DC 00 02 00 62 00 01 00 89 00 02 00 5B 00 .....b.
0000 00F0: 00 00 73 00 01 00 62 00 00 00 5B 00 02 00 B7 00 .....[.
0000 0100: 00 00 C5 00 01 00 E4 00 00 00 6B 00 02 00 02 01 .....k.
0000 0110: 00 00 2E 00 01 00 A7 00 00 00 32 02 02 00 A8 00 .....2.
0000 0120: 00 00 98 00 01 00 20 01 00 00 A8 00 01 00 79 00 .....y.
0000 0130: 00 00 4C 00 01 00 7A 00 00 00 5D 01 01 00 AF 00 ..L...z.
0000 0140: 00 00 CD 00 02 00 89 00 00 00 7A 00 02 00 98 00 .....z.
0000 0150: 00 00 C0 01 02 00 CD 00 00 00 89 00 02 00 C6 00 .....y.
0000 0160: 00 00 98 00 02 00 79 00 00 00 4B 06 01 00 98 00 .....y.
0000 0170: 00 00 89 00 02 00 5B 00 00 00 89 00 02 00 3F 01 .....[.
0000 0180: 00 00 7A 00 01 00 98 00 00 00 4C 00 02 00 C6 00 .....z.
0000 0190: 00 00 5D 01 01 00 D5 00 00 00 89 00 02 00 C5 00 .....[.
0000 01A0: 00 00 03 01 01 00 D5 00 00 00 4C 00 02 00 81 00 .....L.
0000 01B0: 00 00 44 00 02 00 AF 00 00 00 28 04 02 00 54 00 ..D....
0000 01C0: 00 00 A7 00 02 00 C5 00 00 00 54 00 02 00 81 00 .....T.
0000 01D0: 00 00 4C 00 01 00 6B 00 02 00 81 00 00 00 E1 02 ..L...k.
0000 01E0: 01 00 98 00 00 00 63 00 02 00 4C 00 00 00 89 00 .....c.
0000 01F0: 02 00 6A 00 00 00 81 00 02 00 6B 00 00 00 53 00 ..j....
0000 0200: 01 00 54 00 02 00 AF 00 00 00 FF FF FF FF 90 78 ..T....x
0000 0210: 42 A0 54 BA 31 FA 9F 8F A3 B0 4B 35 A9 D5 35 8C B.T.1...K5.5.
0000 0220: 1E 91 C1 E9 04 69 51 4D C6 A8 26 B5 BC E0 D4 66 .....iQM ..&...f
0000 0230: 84 33 81 93 AA EB 95 B1 16 56 0A AF B1 25 9F B4 ..3....V...%..
0000 0240: CC 01 2F 6C 22 4D 09 CA 61 C3 1E 0F 30 C4 84 1B ../l"M. a...0...
0000 0250: E5 E6 A4 0C B2 FA 02 54 60 68 70 A5 CE FF 8A 1A .....T `hp....
0000 0260: 23 1A 5F 0C DB E2 CF B4 A7 E9 51 C2 09 BB 40 CE #. ....Q...@.
0000 0270: D1 06 09 37 8E A9 D5 A4 87 84 2E 58 29 94 92 9C ..7....X)...
0000 0280: 0C 53 AB 05 D2 43 57 AB E1 4D 64 6C 52 93 2A A2 ..S...CW. MdlR.*.
0000 0290: 65 BB 17 E1 CA AB B2 E2 4A 30 BE AB C7 F5 2B 0C e.....J0....
0000 02A0: 86 00 B2 E5 D6 F6 AD 46 87 66 30 30 BE D1 DA F8 .....F .f00....
0000 02B0: 66 28 9D 67 F2 C0 14 C9 18 53 8D 26 E3 D5 A0 4F f(.g....S.&...0
0000 02C0: C2 55 6C 02 C0 88 49 5D D2 44 14 D0 93 81 10 14 ..Ul...I] .D....
0000 02D0: D5 64 78 91 15 5F B9 A5 41 A8 50 27 79 44 F0 DE ..dx... A.P'yD..
0000 02E0: 24 4D 9D 84 19 CE 61 9E 12 BC 5C 32 D1 29 33 63 $M....a. \2.)3c
0000 02F0: 41 E1 91 26 B8 18 33 57 46 93 81 30 EA FF 92 F8 A..&.3W F..0....
0000 0300: 86 BD F0 39 30 D7 41 24 AB 14 F7 87 00 42 44 06 ...90.A$ .....BD.
0000 0310: 08 B8 47 A1 D0 0A A5 9F AE 83 AC 60 3E 8E 25 09 ..G....>.%..
0000 0320: 5D 37 32 ED E7 B2 32 4D 63 06 E2 D3 A8 BE 14 15 |72...2M c.....
0000 0330: A2 A0 EE 30 5E E4 15 7E 79 56 17 30 0C B9 9A 93 ...0^... yV.0....
0000 0340: 3B 93 8A 3A DC A0 58 D8 E3 0F 78 0C D2 FF DA C9 ;...:X. yX....
0000 0350: 84 A1 86 91 42 1F 19 4A 70 2F 3B 38 80 26 A8 49 ....B..J p;/8.&.I
0000 0360: 7D 14 59 78 2A 5D 71 33 A8 A0 44 1D 95 C8 C8 B0 }.Yx*]q3 ..D....
0000 0370: 14 46 01 A8 D8 99 2E A2 0A 1D 25 BC B2 06 94 53 ..F....%.S
0000 0380: 80 8B 41 1C B9 07 09 AD 05 40 41 E2 D6 10 57 FA ..A.....@A...W.
```

- Signed 16bit LE data stored after Mark Table and Silence Detection Table
- Supported sample rate:
 - 16Khz
- Supported bitrates:
 - 16 Kbps
 - 20 Kbps
 - 24 Kbps
 - 28 Kbps
 - 32 Kbps

TeddyRuxpwn

```
usage: teddyruxpwn.py [-h] -i INPUT [-if INPUTFOLDER] [-o OUTPUT]
```

Extract and modify Teddy Ruxpin SNXROM file

optional arguments:

```
-h, --help                show this help message and exit
-i INPUT, --input INPUT    Input snxrom file.
-if INPUTFOLDER, --inputfolder INPUTFOLDER
                           Input snxrom folder.
-o OUTPUT, --output OUTPUT Output Name.
```

TeddyRuxpwn



<http://Defcon26.Exploitee.rs/>

Demo



Thanks

Thank you to the following:

- Exploitee.rs
- Ryan Smith
- DEFCON staff
- My family
- YOU!

HACK ALL THE THINGS!

Come hack hardware with us on IRC:
`irc.freenode.net #Exploitee.rs`