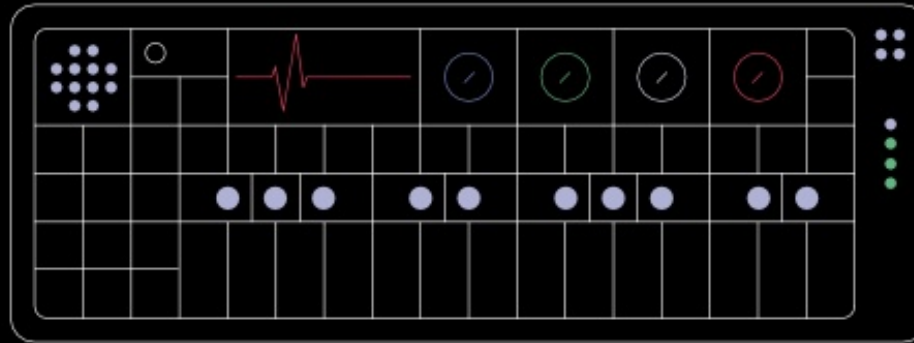
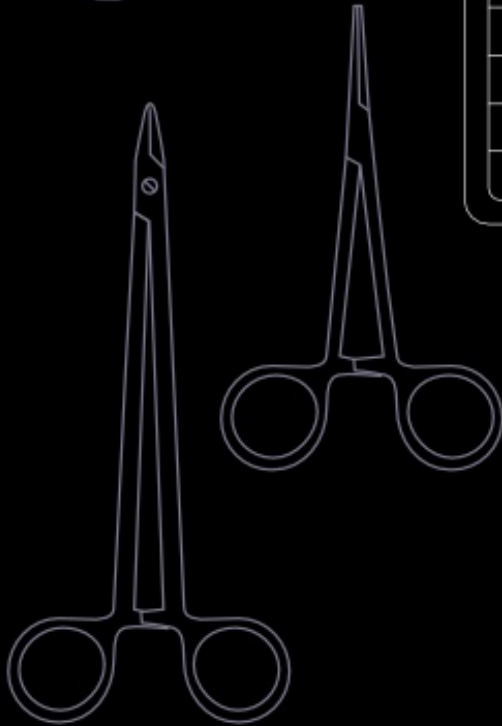


REVERSE ENGINEERING



OP-I



WHO ARE YOU?

- @tabascoeye
 - RaumZeitLabor (Mannheim)
 - The #FaZzZOr Operator
 - NOT a reverse engineer or a security researcher by day
-
- Loves electronic music
 - Enjoys awesome design



WHAT IS THE OP-1



"the portable wonder synthesizer"

- Made by Teenage Engineering in Sweden
- All-in-one portable music production box
- 4-Track tape recorder
- 9 unique synth engines
- Instant sampler (6/12 seconds)
- Multiple sequencers, LFOs, effects
- USB MIDI Controller
- "vector based" amoled display
- Saving power by keeping the screen mostly black

???



THE COOL FEATURES

- Built in accelerometer that can be mapped to basically all parameters (synth engines, effects, adsr curve...)
- Built in FM radio that can be sampled directly
- A Choplifter game
- Amazing graphics:



THE COOL FEATURES

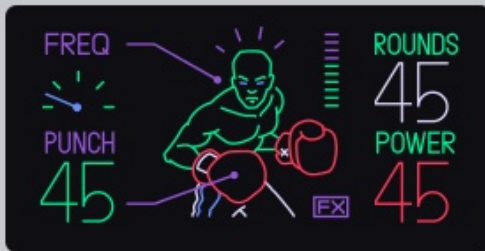
https://teenage.engineering/products/op-1/modules

The image displays a grid of 15 modules from the Teenage Engineering OP-1 synthesizer. Each module has a unique visual theme and controls:

- Module 1:** Features two circular meters, a time display of 2:50:20, and a waveform display.
- Module 2:** Displays four L/R meters, a digital display showing 02 34 45 23, and a MAX EQ button.
- Module 3:** Includes a LOW, MID, and HIGH frequency selector, a CLEAN button, and a MAX EQ button.
- Module 4:** Shows a cow illustration, a FREQUENCY (FREQ) display, a DELAY display, and a SIDEBAND button.
- Module 5:** Features a DETUNE control, a +01 button, and a DRIVE 76 RELEASE 1300 display.
- Module 6:** Includes a DRIVE 76 RELEASE 1300 display, a 20 45 display, and a CC1, CC2, CC3, and CC4 control.
- Module 7:** Shows a graph with a curve, a DRIVE 76 RELEASE 1300 display, and a CC1, CC2, CC3, and CC4 control.
- Module 8:** Features a graph with a curve, a DRIVE 76 RELEASE 1300 display, and a CC1, CC2, CC3, and CC4 control.
- Module 9:** Includes a graph with a curve, a DRIVE 76 RELEASE 1300 display, and a CC1, CC2, CC3, and CC4 control.
- Module 10:** Displays a date and time (2014-04-18 14:27) and a REC, PLAY, STOP, and SIDE control.
- Module 11:** Shows a graph with a curve, a DRIVE 76 RELEASE 1300 display, and a CC1, CC2, CC3, and CC4 control.
- Module 12:** Includes a graph with a curve, a DRIVE 76 RELEASE 1300 display, and a CC1, CC2, CC3, and CC4 control.
- Module 13:** Features a graph with a curve, a DRIVE 76 RELEASE 1300 display, and a CC1, CC2, CC3, and CC4 control.
- Module 14:** Displays a graph with a curve, a DRIVE 76 RELEASE 1300 display, and a CC1, CC2, CC3, and CC4 control.
- Module 15:** Shows a graph with a curve, a DRIVE 76 RELEASE 1300 display, and a CC1, CC2, CC3, and CC4 control.

THE COOL FEATURES

effects



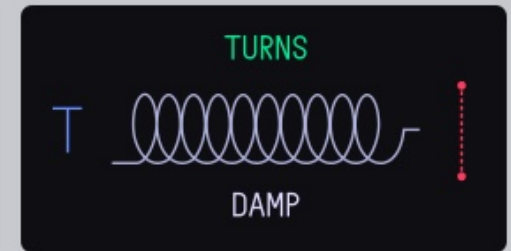
PUNCH
CWO



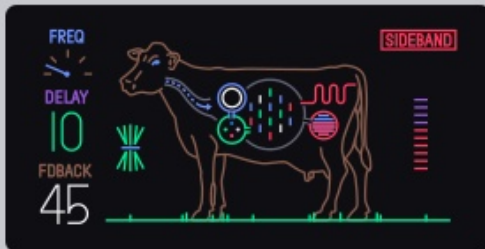
NITRO
PHONE



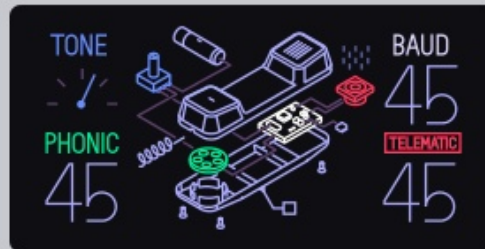
DELAY
GRID



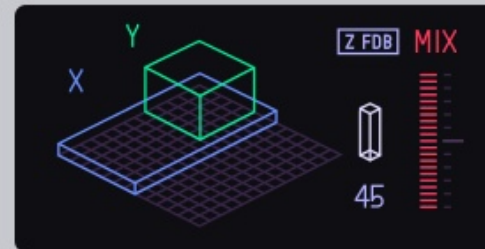
SPRING
EQUALIZER



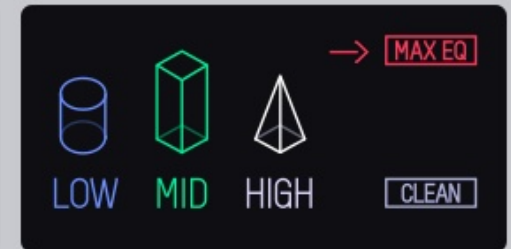
PUNCH
CWO



NITRO
PHONE



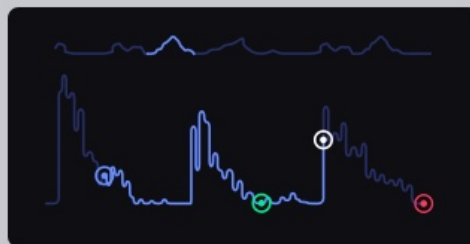
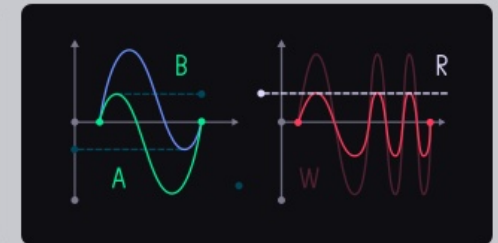
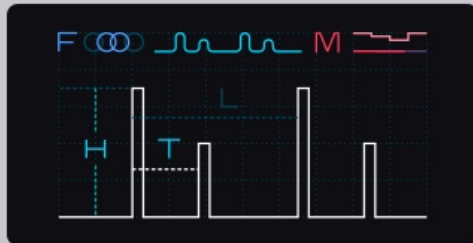
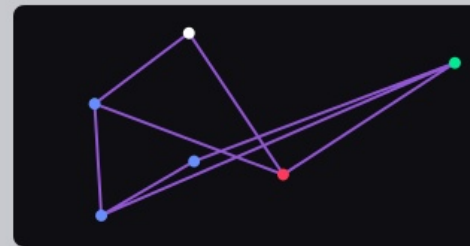
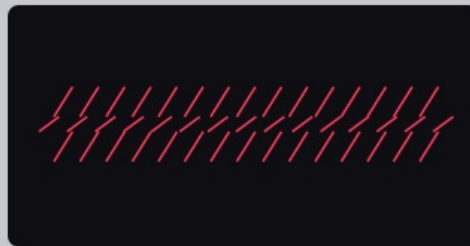
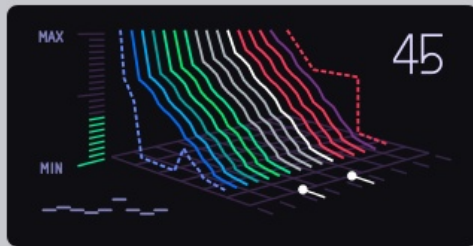
DELAY
GRID



SPRING
EQUALIZER

THE COOL FEATURES

synthesis / samplers



...AND OS UPDATES

- It runs firmware, so it can get updates

HOW TO UPDATE :

- Hold down the COM key before turning the power on.
- This will take you to the "TE-Boot" screen.
- Follow the on-screen instructions.

Updates so far :

- op1_11029.op1 ([ChangeLog](#))
- op1_11082.op1 ([ChangeLog](#))
- op1_11230.op1 ([ChangeLog](#))
- op1_11346.op1 ([ChangeLog](#))
- op1_11381.op1 ([ChangeLog](#))
- op1_11479.op1 ([ChangeLog](#))
- op1_11701.op1 ([ChangeLog](#))
- op1_11855.op1 ([ChangeLog](#))
- op1_12011.op1
- op1_12234.op1
- op1_12469.op1
- op1_12470.op1 ([ChangeLog](#))
- op1_12616.op1 ([ChangeLog](#))
- op1_12788.op1
- op1_13042.op1 ([ChangeLog](#))
- op1_13585.op1 ([ChangeLog](#))
- op1_13747.op1
- op1_14167.op1
- op1_14203.op1 ([ChangeLog](#))
- OP1_AbletonLive_MIDI_Remote_Script.zip



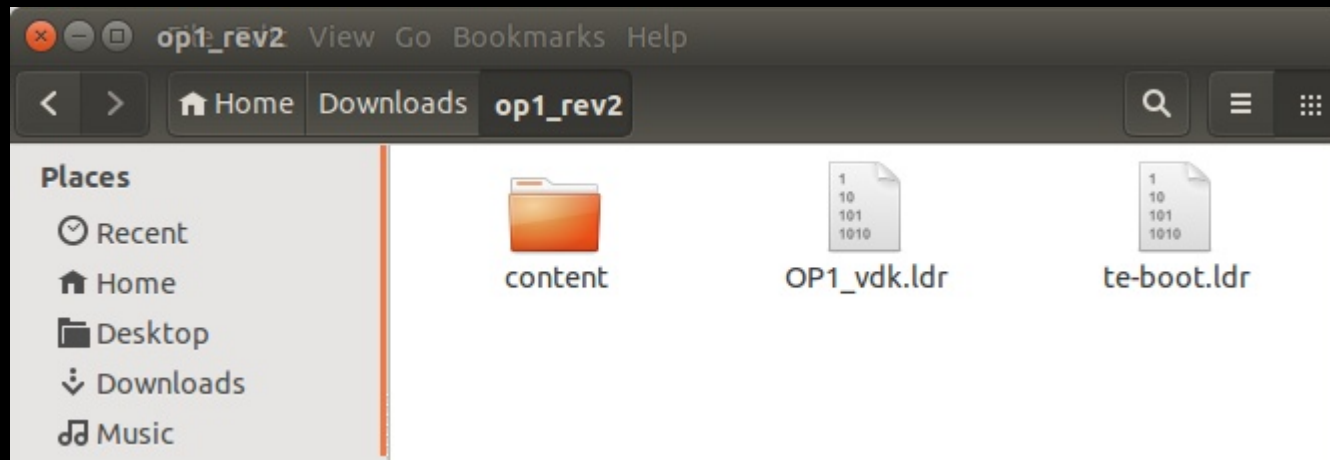
MY HISTORY WITH THE OP-1

- Berlin hipsters need money
 - OP-1s are "affordable" on eBay
 - Bought in May 2014
 - FW Update 14203 came out end of May...
-
- File ending: ".op1"
-
- Let's check that out...



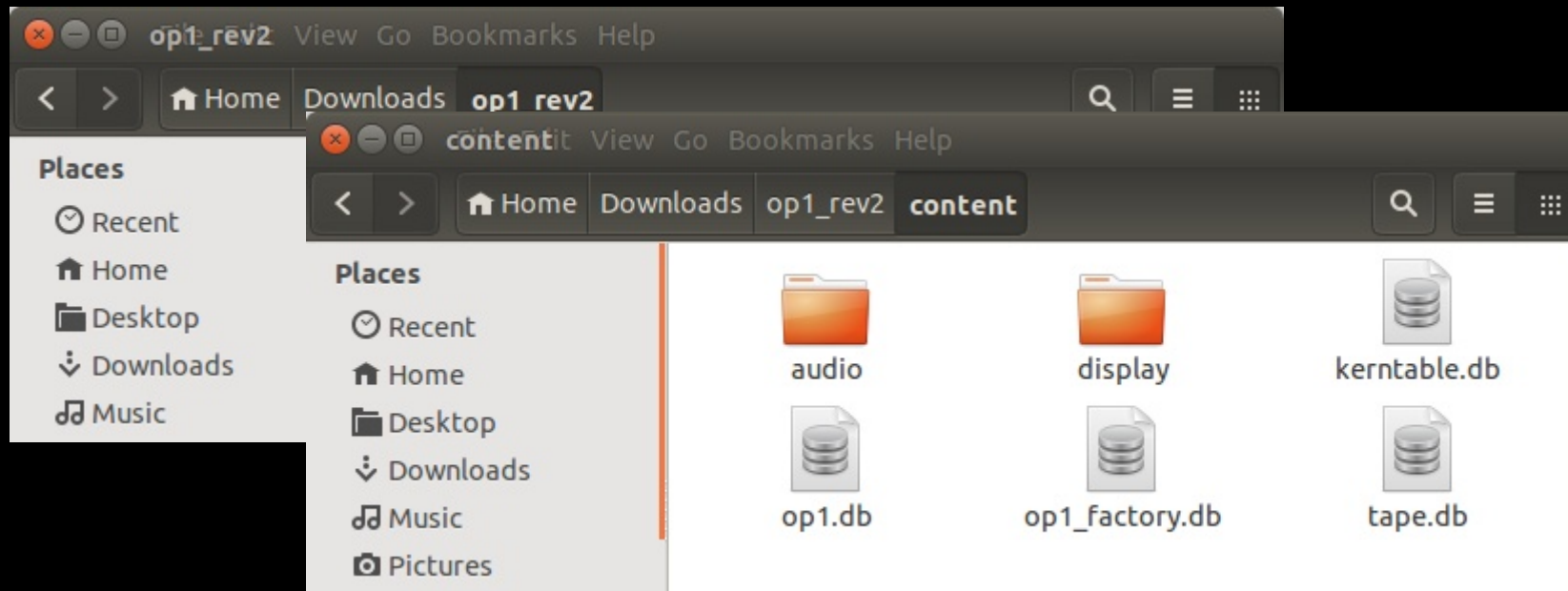
STEP 1: FILE ANALYSIS

- Tip 1: be lazy, use binwalk
- First 4 Bytes == CRC32
- After that: LZMA compressed tar archive

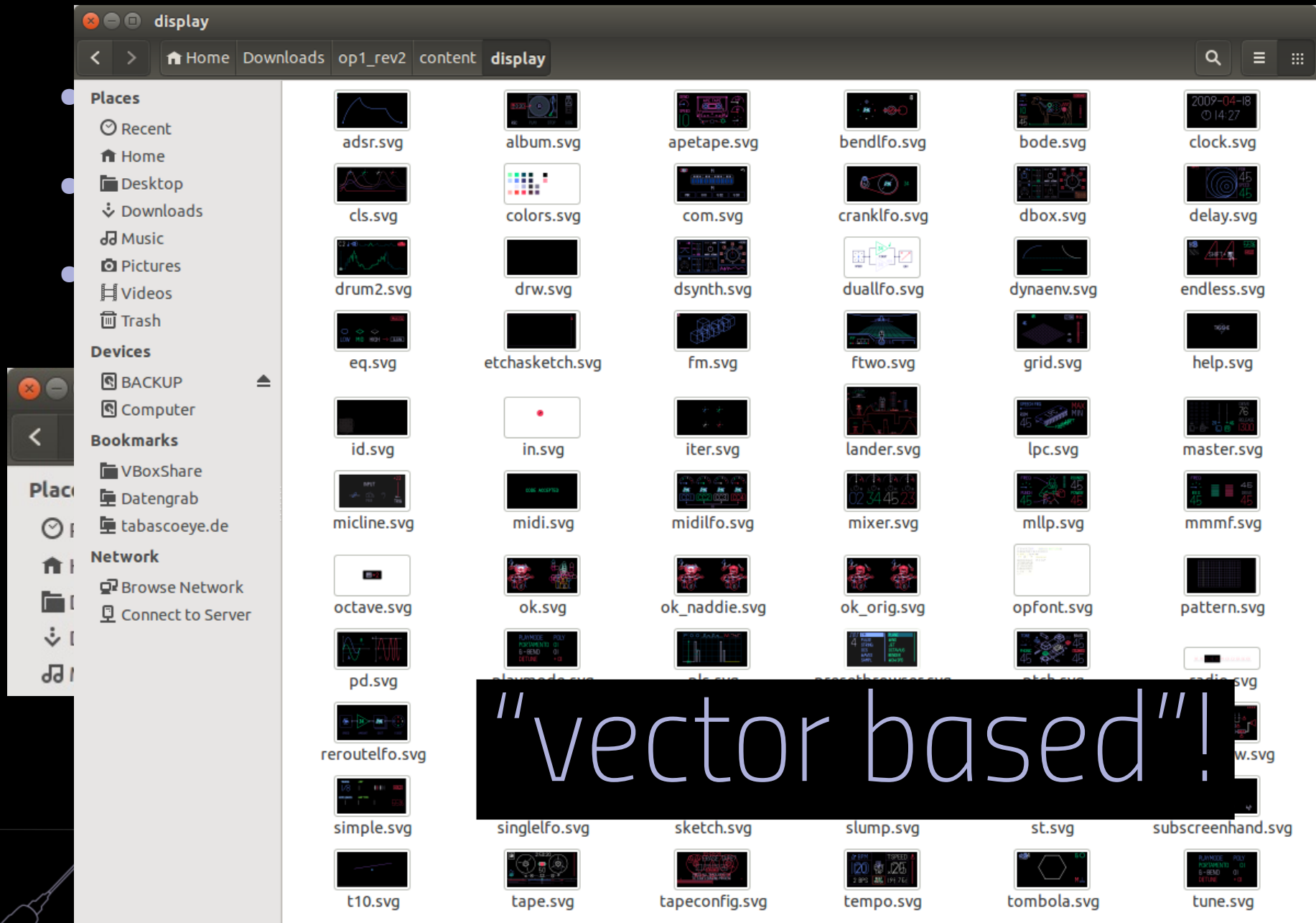


STEP 1: FILE ANALYSIS

- Tip 1: be lazy, use binwalk
- First 4 Bytes == CRC32
- After that: LZMA compressed tar archive



STEP 1: FILE ANALYSIS



MORE ANALYSIS

- More SVGs than seen when using the device...
- The .db files are SQLite databases
- The .ldr files are weird (Ldraw.org ???)



MORE ANALYSIS

SQLite Database Browser - /home/taiba/Downloads/op1_rev

File Edit View Help

Database Structure Browse Data Execute SQL

Table: kerntable

New Record Delete Record

	a	b	kerning
1	v	a	-8.799999
2	a	y	-5
3	l	y	-5.6
4	a	v	-8.399996
5	a	w	-6
6	w	a	-7.800001
7	f	a	-5.6
8	l	t	-10.799998
9	t	c	-1.6
10	a	t	-6.6
11	t	a	-8.8
12	t	q	-2.4
13	q	t	-3
14	t		4 -6.2
15		5	5 -2.200001
16	?	?	7.200002
17		1 :	3.8
18	:		1 4.2
19	1		1 7.8

< 1 - 73 of 73 > Go to: 0

MORE ANALYSIS

SQLite Database Browser - /home/taiba/Downloads/op1_rev/content/op1_factory.db

File Edit View Help

Database Structure Browse Data Execute SQL

Table: fx_types

New Record Delete Record

	id	type	default_params
1	3	grid	[8000, 8000, 18000, 18000, 8000, 8000, 8000, 8000]
2	4	punch	[6000, 15000, 20000, 28000, 8000, 8000, 8000, 8000]
3	5	delay	[8000, 8000, 8000, 8000, 0, 0, 0, 0]
4	7	phone	[8000, 8000, 8000, 16000, 8000, 8000, 8000, 8000]
5	8	spring	[8000, 15000, 2000, 20000, 8000, 8000, 8000, 8000]
6	9	cwo	[5000, 8192, 16384, 32767, 0, 0, 0, 0]
7	10	nitro	[500, 0, 10500, 16000, 0, 0, 0, 0]

< 1 - 7 of 7 >

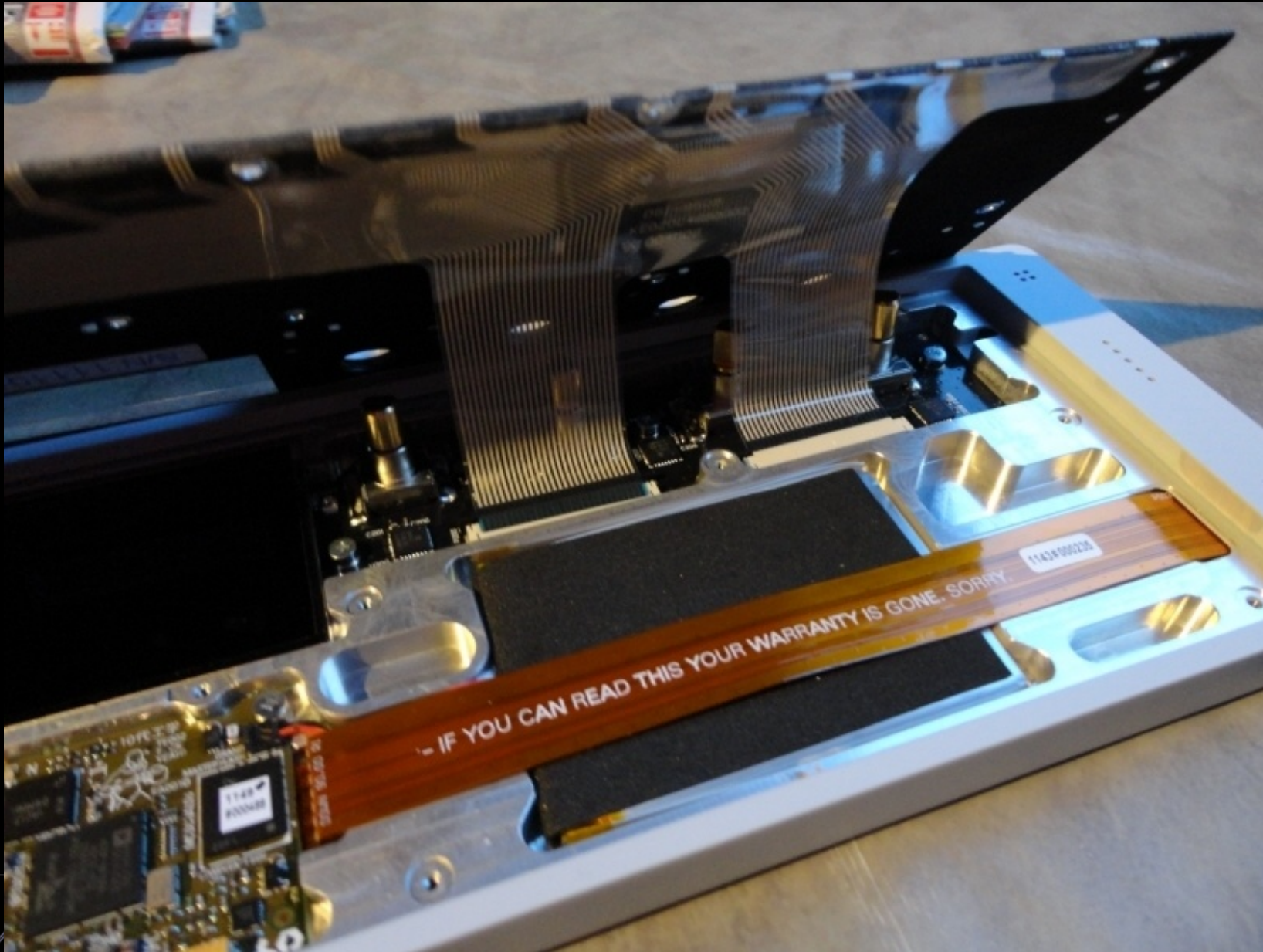
Go to: 0

STEP2: GATHER MORE INTEL

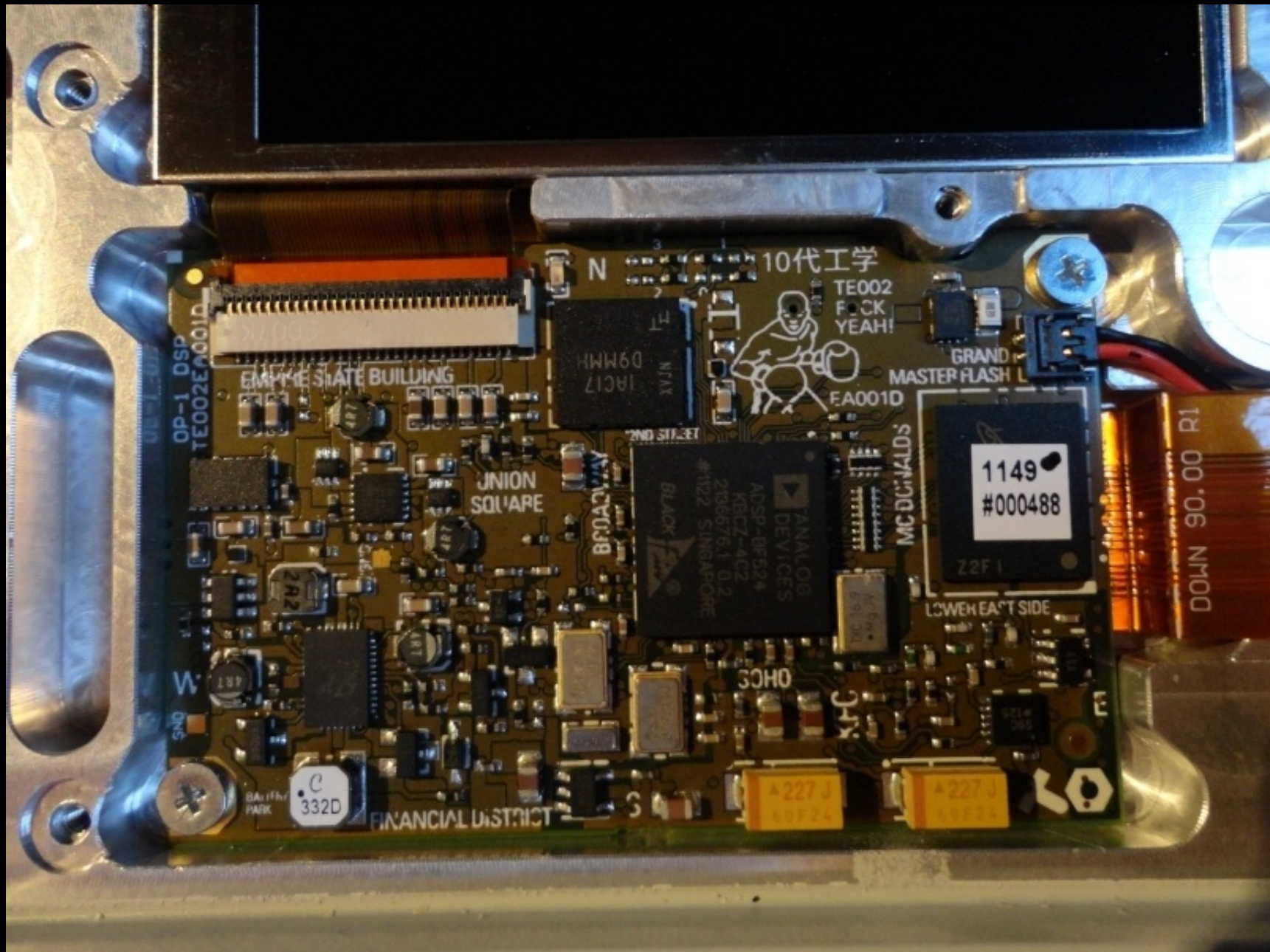
- Found beautiful pictures of the OP-1 PCBs
- CPU is Analog Devices BlackFin DSP (BF-524)



STEP2: GATHER MORE INTEL



STEP2: GATHER MORE INTEL



BlackFin DSPs

- Also used in Rigol Oscilloscopes (DSO)
- 16/32 bit instructions
- Parallel instructions
- LockBox security features (secure boot? Signed FW?)
- Runs ucLinux or VisualDSP++/VDK
- Boot process uses "loader" files ==> .ldr

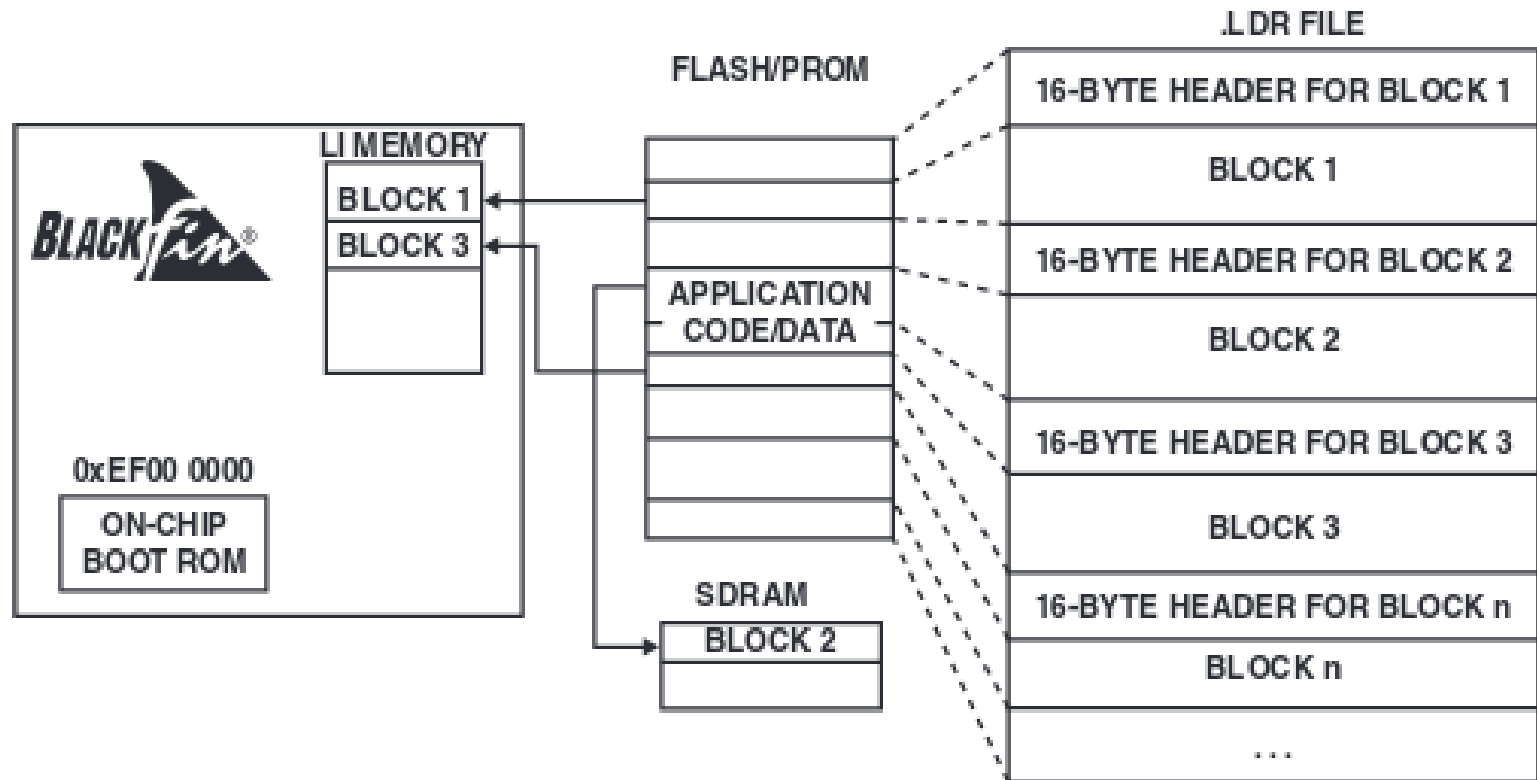


LDR Format

- Actually, not LEGO...
- Somewhat compressed file
- Blocks with headers to tell the CPU type of block and load to which memory address in the mem map
- Some blocks have "fill" flag but no data: "compression"
"Fill the area from 0x123 with 200 zeros/ones"



LDR Format



MY CRUDE PYTHON SKILLZ

- Still thinking this runs ucLinux...
- Started to write a crude "decompressor" in python
- Idea: turn the LDR back into an DXE executable
- People on forums describe DXE as "like ELF"
- Should be able to use with radare2 or similar?
- Github: <https://github.com/tabascoeye/ldr2dxe>
- August 2014
- Lost interest for a while...




2 YEARS LATER

musikmesse

7. – 10. April 2016

musikmesse.com

It's my tune.

 messe frankfurt



MUSIKMESSE 2016

- Teenage Engineering shows BETA of a new OS
- Fan Forum (Operator-1.com) explodes
- Beta is subsequently leaked somehow



STEP 3: GET MOTIVATION AND HELP

- Posted a diff of 14203 and 076 on Forum
- Some SVGs gone, some new ones
- First try at re-packing the FW with correct CRC
- Upload succeeded
- Played around with some SVG files
- => first publicly known custom FW on the OP1 (I think)



STEP 3: GET MOTIVATION AND HELP

Compare ↑ ↓ × Copy Left Copy Right Delete Same New Modified Filters ▾

[_op1_14203.op...ed]_4.extracted ✕

/home/taiba/Downloads/_op1_14203.op1.extracted/_4.extracted ▾ Browse...

Name	Size	Modification time
▼ _4.extracted	4.1 kB	Fr 02 Sep 2016 20:08:32
▼ content	4.1 kB	Di 25 Mär 2014 00:26:01
▼ audio	4.1 kB	Fr 06 Dez 2013 09:53:49
▶ drum	4.1 kB	Fr 06 Dez 2013 09:53:48
▶ factory_drum	4.1 kB	Fr 06 Dez 2013 09:53:53
▶ factory_synth	4.1 kB	Fr 06 Dez 2013 09:53:49
▶ preset_drum	4.1 kB	Fr 06 Dez 2013 09:53:48
▶ preset_synth	4.1 kB	Fr 06 Dez 2013 09:53:48
▶ speech	4.1 kB	Fr 06 Dez 2013 09:53:48
▶ synth	4.1 kB	Fr 06 Dez 2013 09:53:46
▼ display	12.3 kB	Do 13 Mär 2014 18:34:40
chor.svg	12.2 kB	Fr 06 Dez 2013 09:53:55
delay.svg	8.8 kB	Fr 06 Dez 2013 09:53:55
duallfo.svg	10.5 kB	Fr 06 Dez 2013 09:53:55
iter.svg		
simple.svg		
slump.svg		
tempo.svg	20.9 kB	Fr 06 Dez 2013 09:53:55
op1.db	88.1 kB	Fr 06 Dez 2013 09:53:55
op1_factory.db	92.2 kB	Di 25 Mär 2014 00:26:01
OP1_vdk.ldr	2.1 MB	Di 15 Apr 2014 10:16:53
te-boot.ldr	239.1 kB	Mi 22 Jan 2014 11:32:36

/home/taiba/Downloads/_op1_076.op1.extracted/_4.extracted ▾ Browse...

Name	Size	Modification time
▼ _4.extracted	4.1 kB	Fr 02 Sep 2016 20:08:05
▼ content	4.1 kB	Di 22 Mär 2016 14:36:36
▼ audio	4.1 kB	Do 24 Mär 2016 10:28:08
▶ drum	4.1 kB	Di 22 Mär 2016 14:36:36
▶ factory_drum	4.1 kB	Di 22 Mär 2016 08:56:50
▶ factory_synth	4.1 kB	Mo 21 Mär 2016 19:24:36
▶ preset_drum	4.1 kB	Do 24 Mär 2016 10:28:08
▶ preset_synth	4.1 kB	Do 24 Mär 2016 10:28:08
▶ speech	4.1 kB	Mo 21 Mär 2016 19:24:36
▶ synth	4.1 kB	Di 22 Mär 2016 14:36:36
▼ display	12.3 kB	Mo 21 Mär 2016 19:24:36
chor.svg		
delay.svg	8.7 kB	Mo 21 Mär 2016 19:24:36
duallfo.svg	10.5 kB	Mo 21 Mär 2016 19:24:36
iter.svg	4.1 kB	Mo 21 Mär 2016 19:24:36
simple.svg	13.5 kB	Mo 21 Mär 2016 19:24:36
slump.svg	4.0 kB	Mo 21 Mär 2016 19:24:36
tempo.svg	21.6 kB	Mo 21 Mär 2016 19:24:36
op1.db	36.9 kB	Di 22 Mär 2016 14:36:36
op1_factory.db	97.3 kB	Di 22 Mär 2016 08:56:50
OP1_vdk.ldr	2.1 MB	Do 24 Mär 2016 10:40:20
te-boot.ldr	241.1 kB	Mo 21 Mär 2016 19:28:02

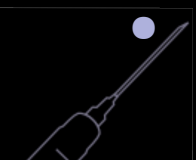
rwxr-xr-x 34 months

STEP 3: GET MOTIVATION AND HELP



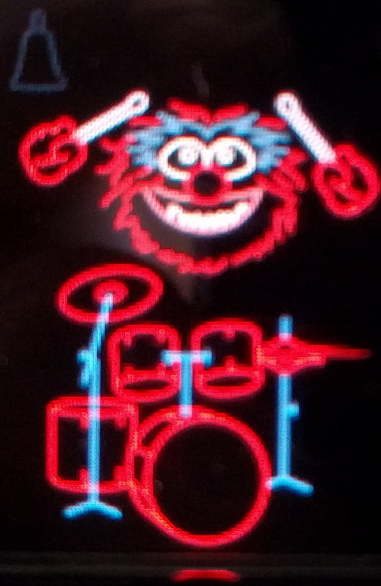
STEP 3: GET MOTIVATION AND HELP

- New topic opened on Forum: "Custom Firmware"
- Starting with a public disclaimer to TE (!)
- Details of Firmware (SQLite DBs, LDR files, SVGs)
- Opensource libs discovered in LDR via 'strings':
 - Yaffs2, libaiff-5.0, sqlite 3, box2d, libjson...
- Understanding the SVG concept
 - Adobe Illustrator CS4, CS5, creative cloud
 - "Animations" mainly done with toggling "display=none"
 - Groups and IDs must be preserved (Inkscape kills most of it?)
- First cool graphics mods thanks to @flederrattie

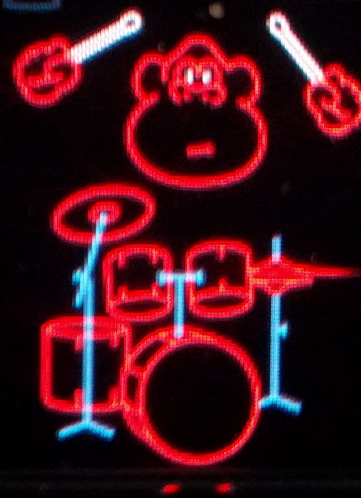


Block 96 → ignore

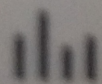
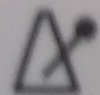




HOLD



JOIN



1

2

3

4

STEP 3: GET MOTIVATION AND HELP

- Rambling about the missing IDs in `fx_type` table
- Trying out some values for "filter" but get crashes: "invalid parameter value"
- Waking up to message from Wavi (kudos!)
- He unlocked "filter" FX by copying parameters from another fx



FREQ



RES

66



HP IV

DRIVE



1

2

3

4

STEP 3: GET MOTIVATION AND HELP

- New synth engine "Iter" unlocked
- Only exists in the beta, not finished at all
- Just like the other new synth in the beta: no graphics
- No luck with other "missing" FX types:
 - Apetape
 - Lpc
 - Chorus
- Maybe wrong name or missing in the FW?
- ==> Let's get dirty with the LDR files...



STEP 3: GET MOTIVATION AND HELP

- Discussions on IDApro BlackFin plugin by codenaschen
<https://github.com/krater/Blackfin-IDA-Pro-Plugin>
- Made for Visual Studio 6 and older IDA SDK
- Woke up to a working fork of IDApro plugin made by JakeOkay (kudos!)

- And this:

From teenage engineering <support@teenage.engineering>★
Subject **OP-1 custom firmware**
To tabascoeye@gmail.com★

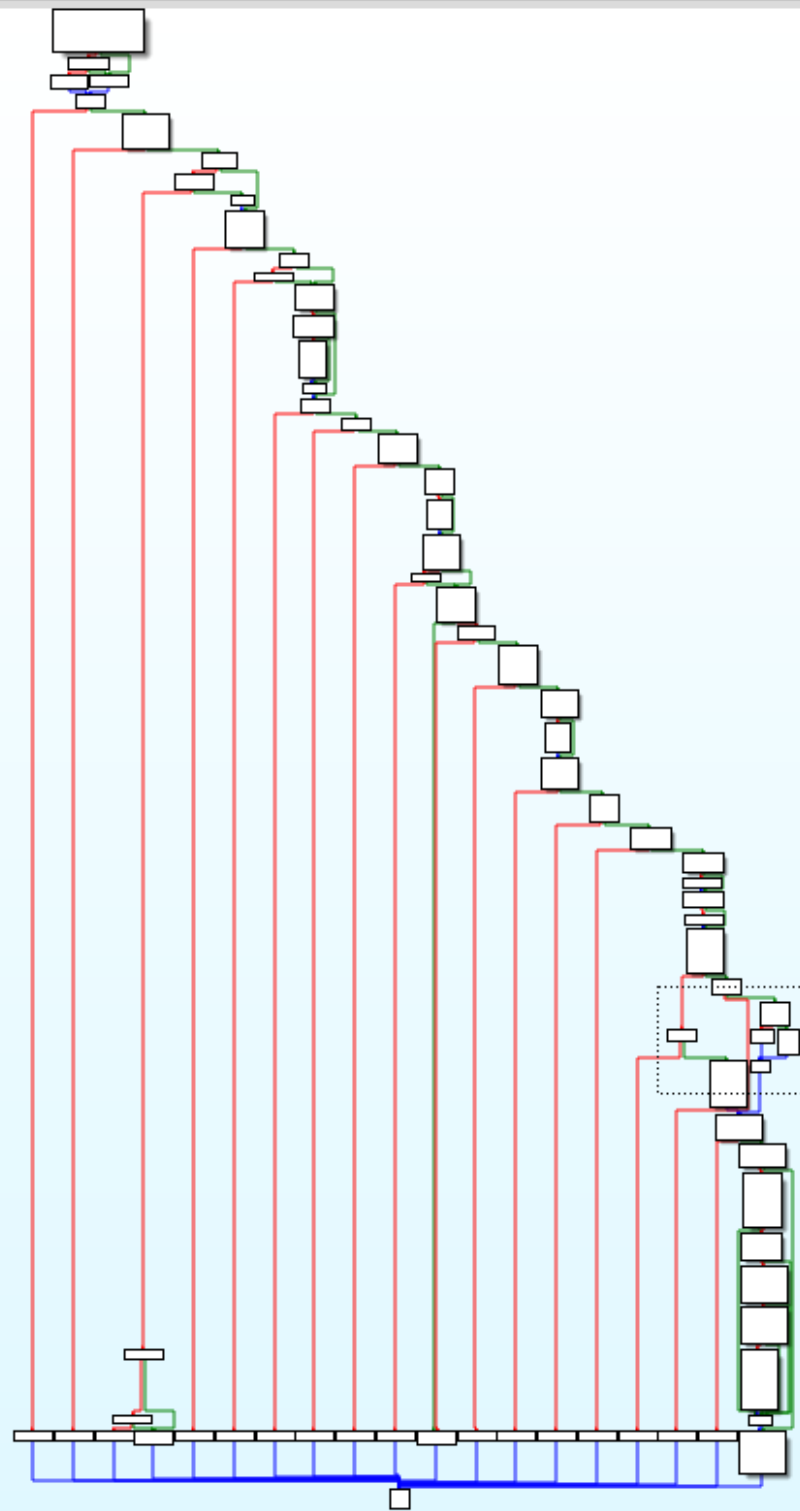


[illegible]

STEP4: GREETINGS, IDA

- pretty steep learning curve
- Especially with a custom processor plugin (i.e. no x86)

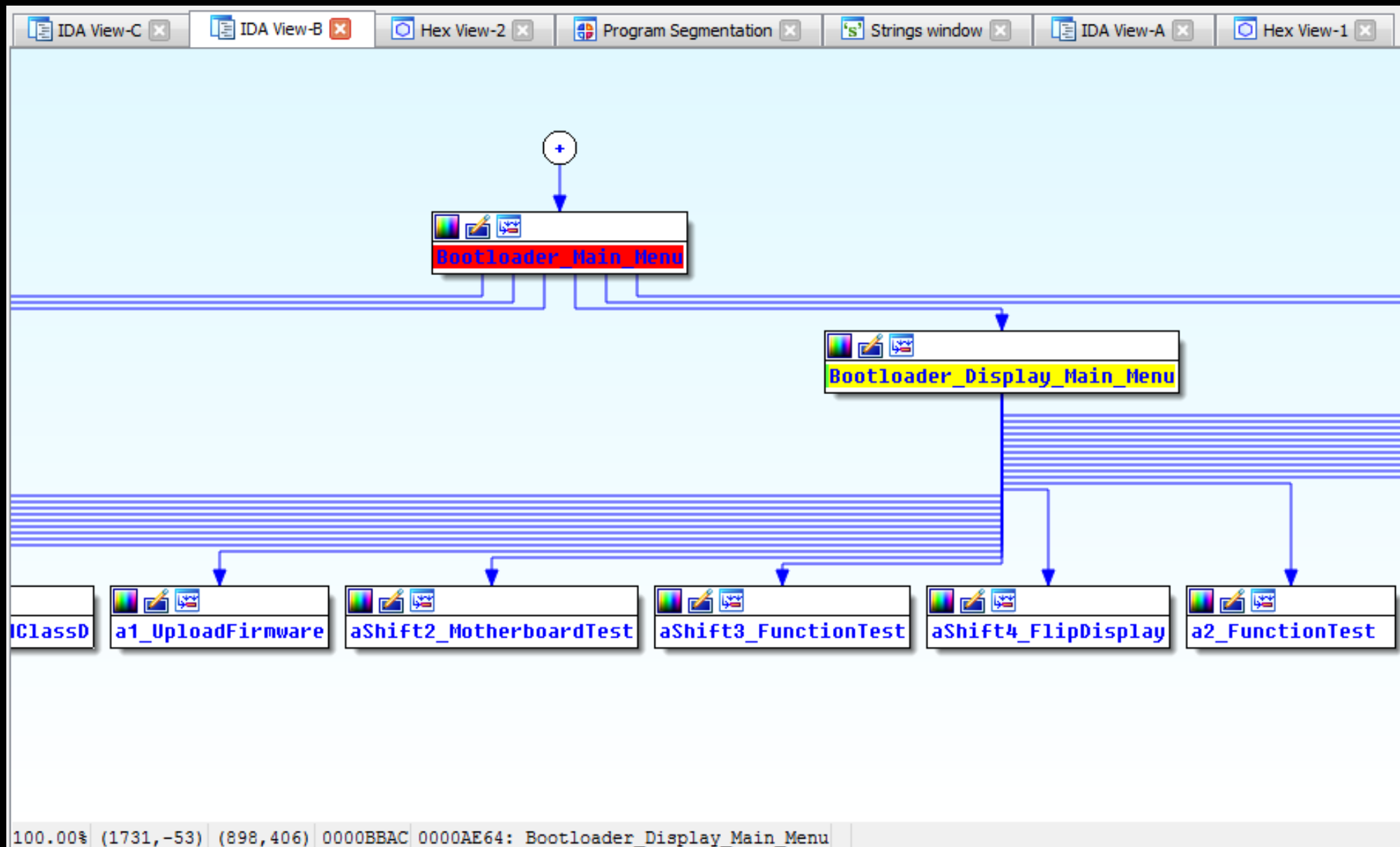




te-boot.ldr VS OP1_vdk.ldr

- Bootloader is parsed fine
- Main OS does not parse with our plugin
- Too many “illegal” instructions
- Analysis+Naming via:
 - Referenced strings
 - Called functions and proximity browser
 - CPU Manual (ROM functions etc.)





Windows7 (RetinaEngrave 4.4.0.7) [Running] - Oracle VM VirtualBox

Machine View Devices Help

IDA - C:\Users\Fabian\Downloads\OP-1_rev\te-boot.idb (te-boot.idb)

File Edit Jump Search View Options Windows Help

Library function Data Regular function Unexplored Instruction External symbol

Functions window

sub_16BF6

DATA1:FF807FFE
DATA2:FF900000 # =====
DATA3:FF800000

Address

FINDINGS IN BOOTLOADER

- Hidden Developer(?) Menu
- Depending on a value in OTP Memory of CPU
- ==> developer OP1s have magic value in there?
- One-Time Programmable?
 - Once a dev OP1, forever a dev OP-1?
- The "OT" part of OTP is not that strict on BlackFins according to the Manual
- CAN be locked via command ==> never writeable again



IDA View-C x IDA View-B x Hex View-2 x Program Segmentation x Strings window x IDA View-A x Hex View-1 x

```
R0.L = 0x5dcc;      # R0=0xFF805dcc
R0.H = 0xFF80;      # R0=0xFF805dcc
                    -> a1_UploadFirmware -> "1. Upload Firmware"
CALL display_text;
P1.L = 0x2be9;      # P1=0xFF802be9
P1.H = 0xFF80;      # P1=0xFF802be9
                    -> unk_FF802BE9
R0 = B[P1] (2);
CC = (R0 == 0x0);
IF !CC JUMP loc_AF20; # R0=0xFF805e30
```

0; # R0=0xFF805de0
0; # R0=0xFF805de0
-> aShift2_MotherboardTest -> "shift + 2. Motherboard test"
text;
0; # R0=0xFF805dfc
0; # R0=0xFF805dfc
-> aShift3_FunctionTest -> "shift + 3. Function test"
text;
0; # R0=0xFF805e18
0; # R0=0xFF805e18
-> aShift4_FlipDisplay -> "shift + 4. Flip Display"
text;
3C; # R0=0xFF805e44

loc_AF20: # R0=0xFF805e30
R0.L = 0x5e30; # R0=0xFF805e30
R0.H = 0xFF80; # R0=0xFF805e30
-> a2_FunctionTest -> "2. Function test"
CALL display_text;
R0 = ROT R7 BY 0x0;
CALL display_text;
R0 = ROT R7 BY 0x0;
CALL display_text;

loc_AF3C: # R0=0xFF805e44
R0.L = 0x5e44; # R0=0xFF805e44
R0.H = 0xFF80; # R0=0xFF805e44
-> a7_FactoryReset -> "7. Factory reset"
CALL display_text;
R0.L = 0x5e58; # R0=0xFF805e58
R0.H = 0xFF80; # R0=0xFF805e58
-> a8_FormatDrive -> "8. Format drive"
CALL display_text;
R0 = ROT R7 BY 0x0;

80.00% (102,1042) (886,302) 0000BC0E 0000AEC6: Bootloader_Display_Main_Menu+62

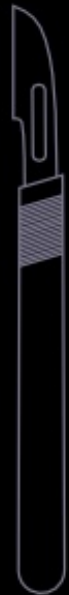
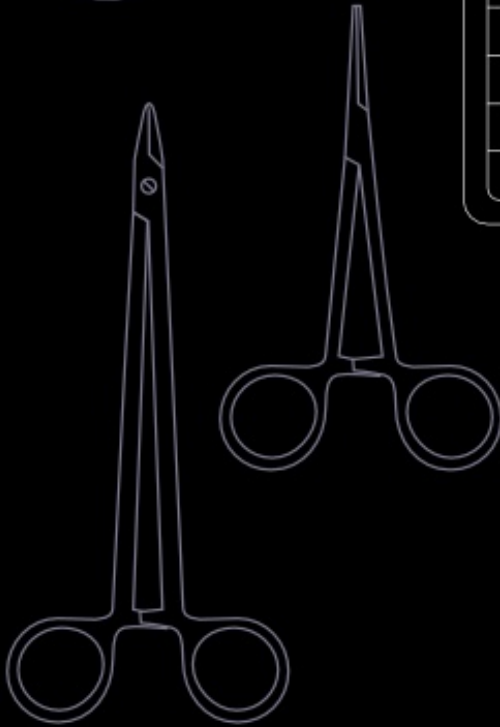
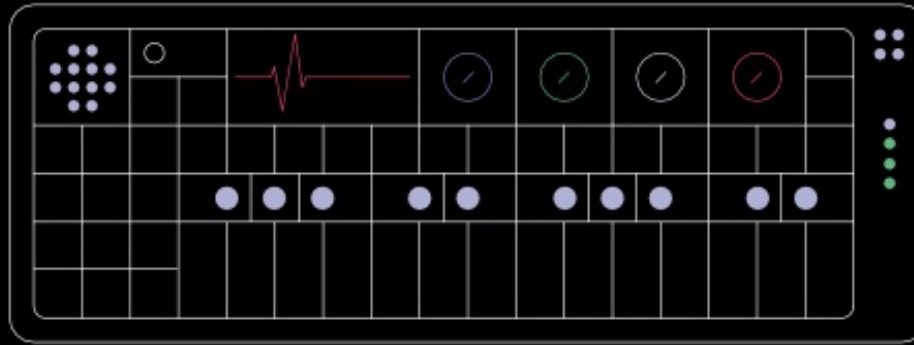
13GB

TODO AND THANKS

- The IDA plugin needs work AND/OR
- Someone introduces me to radare2 plugin writing
- TODO:
 - Get OP1_vdk.ldr to parse correctly
 - Find out what happened to lpc, apetape, chrous
 - Come up with some more awesome graphic mods
 - Modify the choplifter game ;o)
- THANKS:
 - Wavi (aka @riichrd), jakeokay (aka @clpwn), @flederrattie, everyone on operator-1.com and of course Teenage Engineering for this amazing device



QUESTIONS?



SOME LINKS TO GUIDE YOU

- teenage.engineering – company website
- Forums
 - Operator-1.com – great fan forum
 - Subreddit OP1users
- Sample packs and other stuff
 - Go-p1.net – nice page with resources, links, samples...
 - op1essentials.com – sample packs (most of them paid)
- Misc
 - noorden.org/op1/ – first OP-1-only-compilation
 - store.professorkliq.com/album/28-days-with-the-op-1

