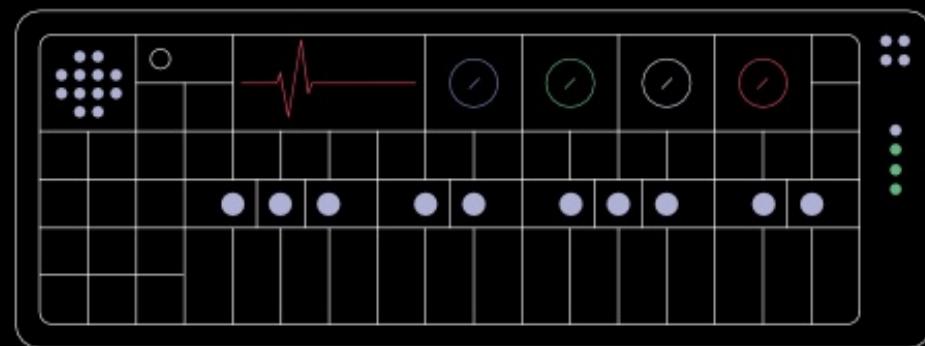
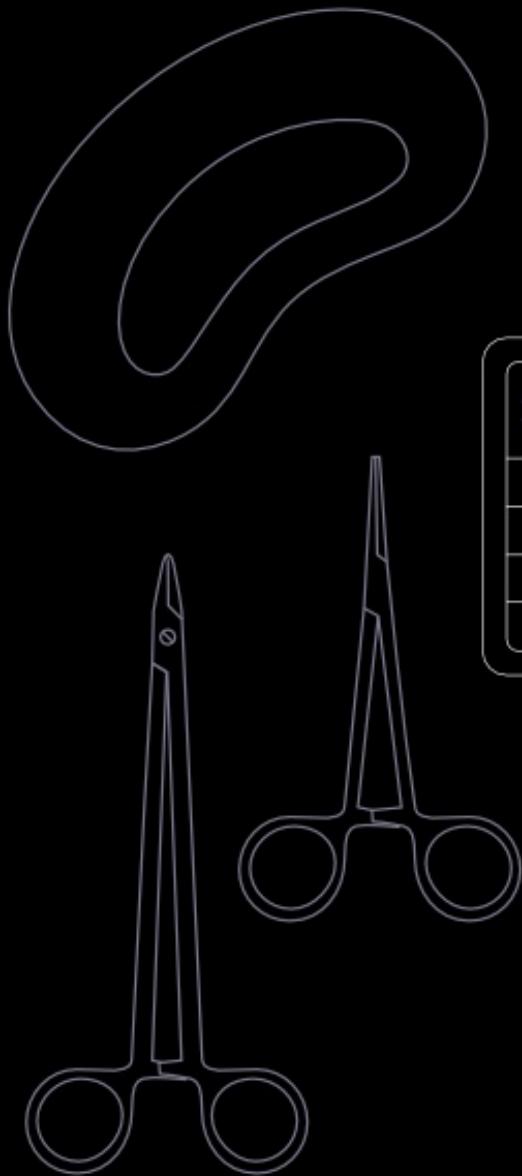


REVERSE ENGINEERING



OP-|



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



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

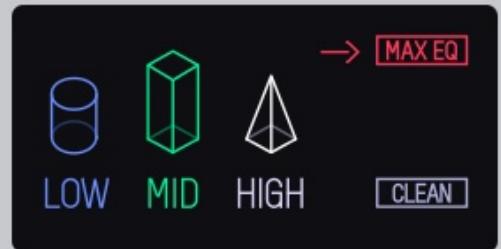
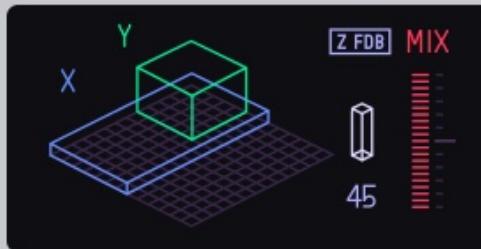
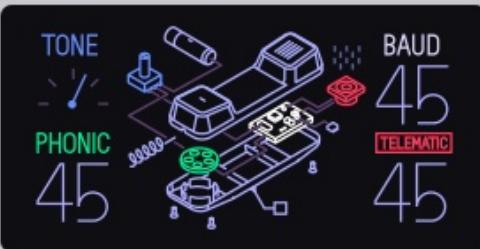
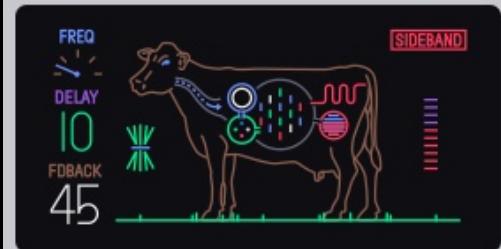
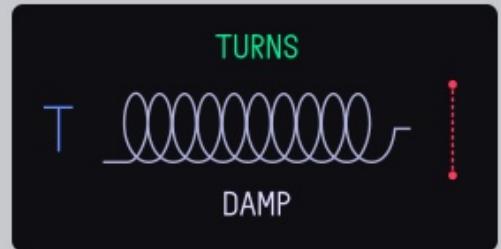
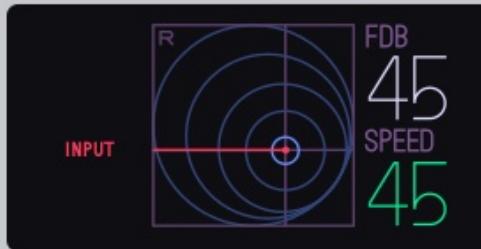
https://teenage.engineering/products/op-1/modules

The image displays a grid of 16 modules from the Teenage Engineering OP-1 synthesizer, each with a unique and visually appealing interface. The modules are arranged in four rows and four columns.

- Row 1:**
 - Module 1: A circular control panel with four knobs labeled 1, 2, 3, and 4, and a digital display showing "2:50:20".
 - Module 2: A digital display showing a sequence of numbers: 02, 34, 45, 23.
 - Module 3: A graphic equalizer with three bands labeled LOW, MID, and HIGH, and a "CLEAN" button.
 - Module 4: An illustration of a cow's head with various waveforms and parameters like FREQ, DELAY, and FBK.
- Row 2:**
 - Module 1: A digital display showing "DETUNE +01".
 - Module 2: A digital display showing "DRIVE 76 RELEASE 1300".
 - Module 3: Four circular controls labeled CCI, CC2, CC3, and CC4, each with a small icon above it.
 - Module 4: A graph showing a green curve with a sharp peak and a long tail.
- Row 3:**
 - Module 1: A complex circuit diagram involving LFOs, filters, and drive sections.
 - Module 2: A digital display showing the date "2014-04-18" and time "14:27".
 - Module 3: A turntable-style interface with buttons for REC, PLAY, STOP, and SIDE, and a digital display showing "0:20".
 - Module 4: A digital display showing "JUJ 4 FM PLANE" with a list of sound types: PULSE, WIND, STRING, JET, OCS, WAVES, OCTAVIUS, BENDER, SAMPL, and WOW SPD.
- Row 4:**
 - Module 1: A digital display showing "INPUT +23" with a TRIG input symbol.
 - Module 2: A graph showing a smooth, rounded curve.
 - Module 3: A connection diagram between an OP-1 module and a computer via USB, with buttons for DISK MODE, OP-1, MIDI, DISK, and OPT.
 - Module 4: A large green button labeled "STANDBY" with a power icon below it.
- Row 5:**
 - Module 1: A digital display showing "PLAYMODE POLY PORTAMENTO 01".
 - Module 2: A digital display showing "RECORDING!" with a sunburst icon below it.
 - Module 3: A detailed illustration of a city skyline with various buildings and structures.
 - Module 4: A blank black space.

THE COOL FEATURES

effects



PUNCH
CWO

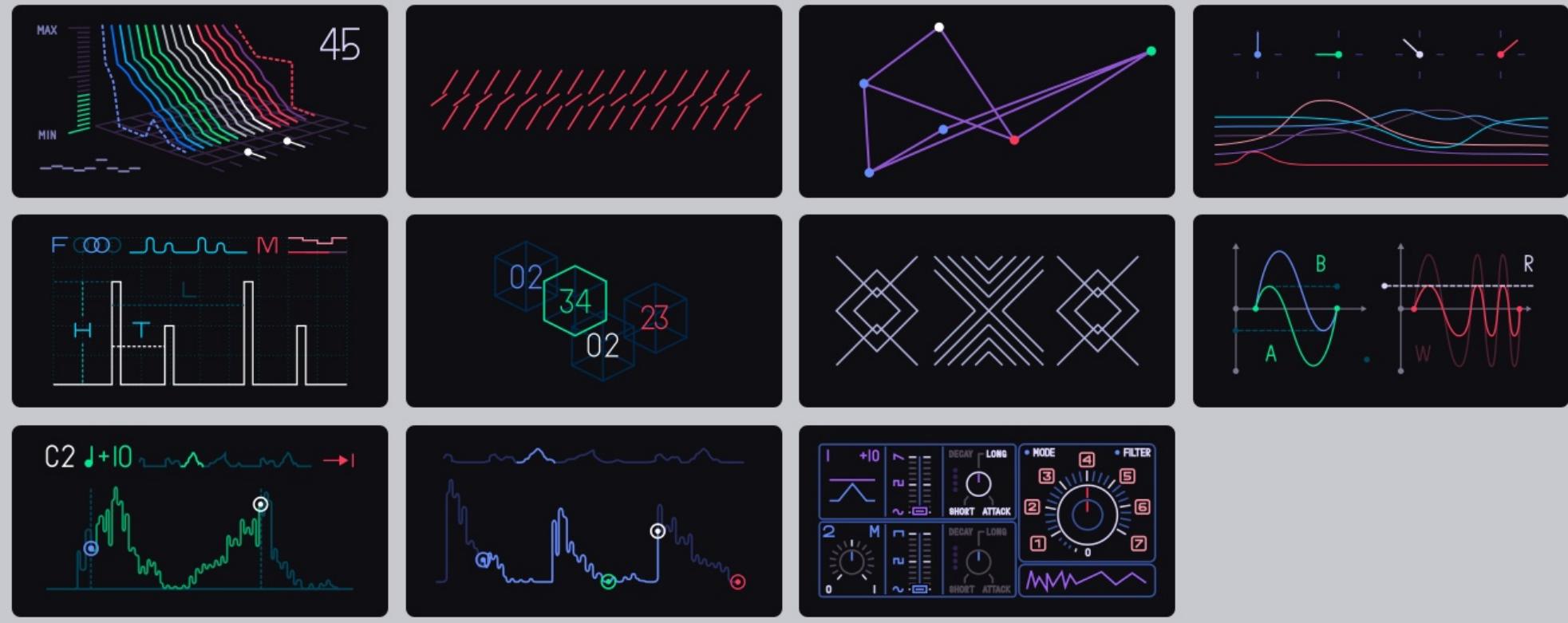
NITRO
PHONE

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

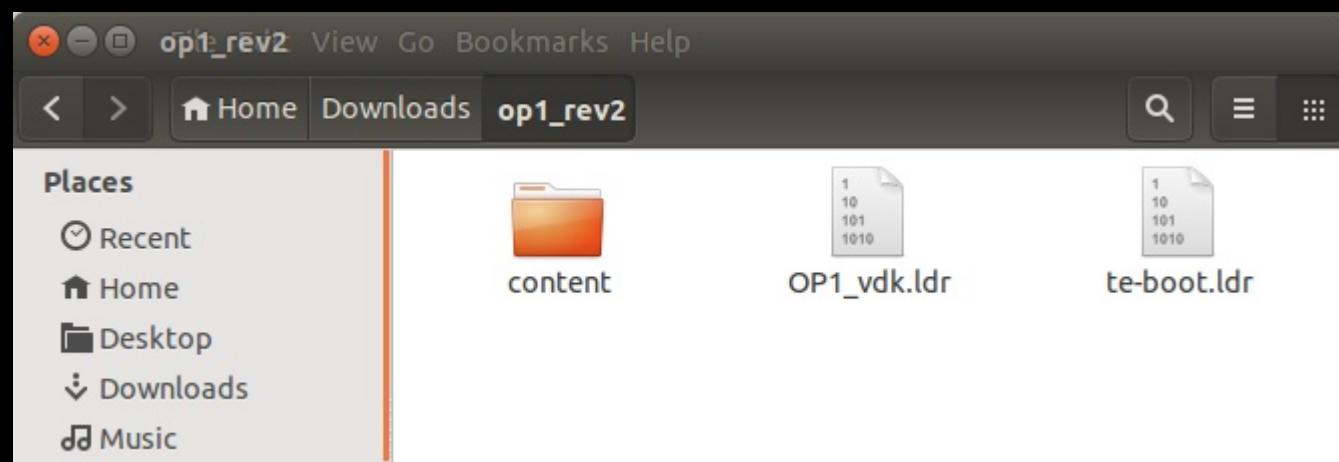
MY HISTORY WITH THE OP-1

- 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...



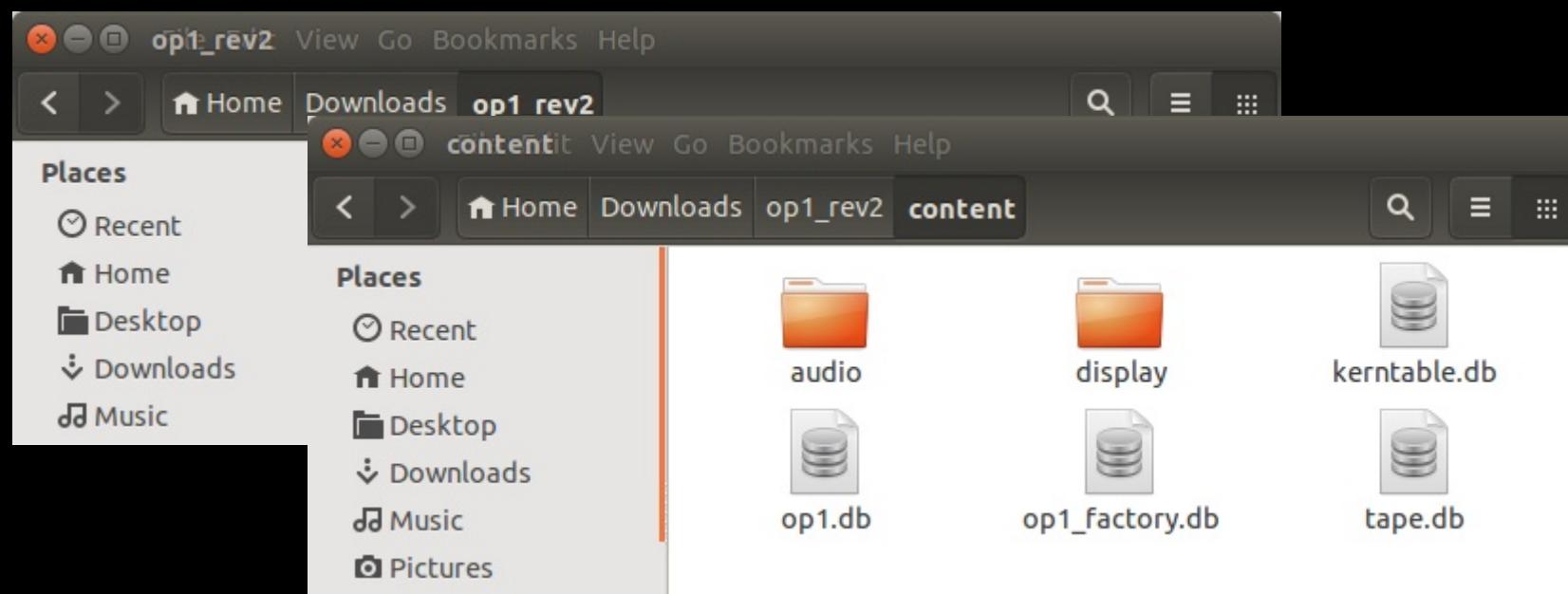
STEP 1: FILE ANALYSIS

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

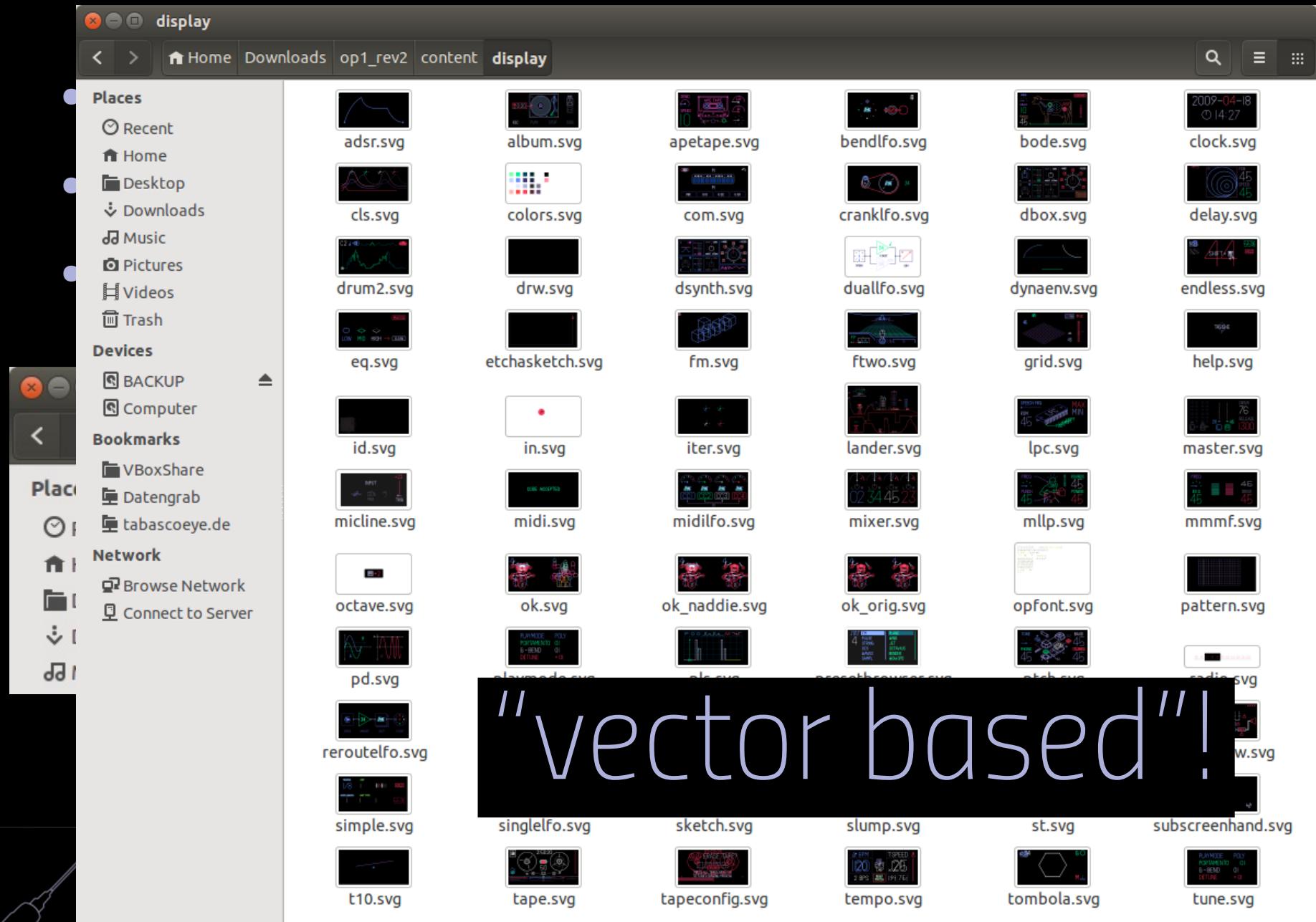


STEP 1: FILE ANALYSIS

- 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/taba/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
15		5	-6.2
16	?	?	5
17		1:	-2.200001
18	:		7.200002
19	+		3.8
		1	4.2
		1	7.9

< 1 - 73 of 73 > Go to: 0

MORE ANALYSIS

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

File Edit View Help

Database Structure Browse Data Execute SQL

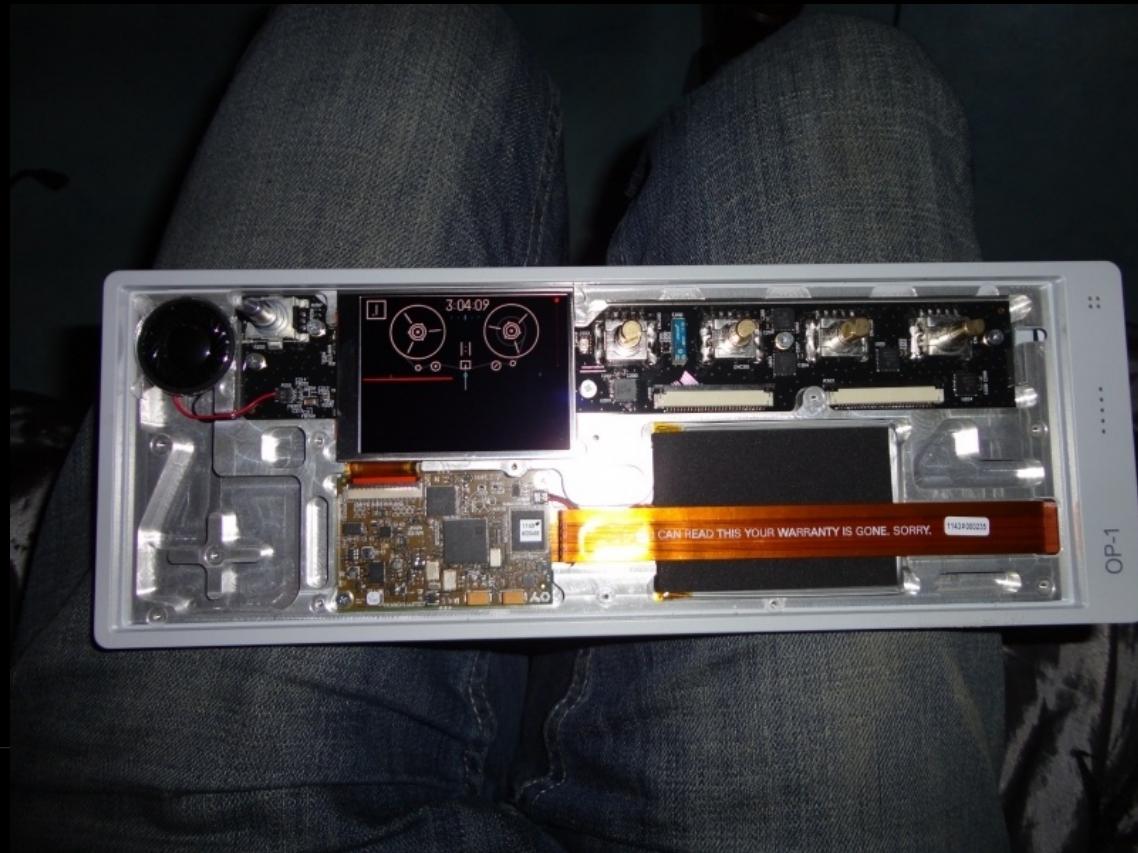
Table: fx_types New Record Delete Record

	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]

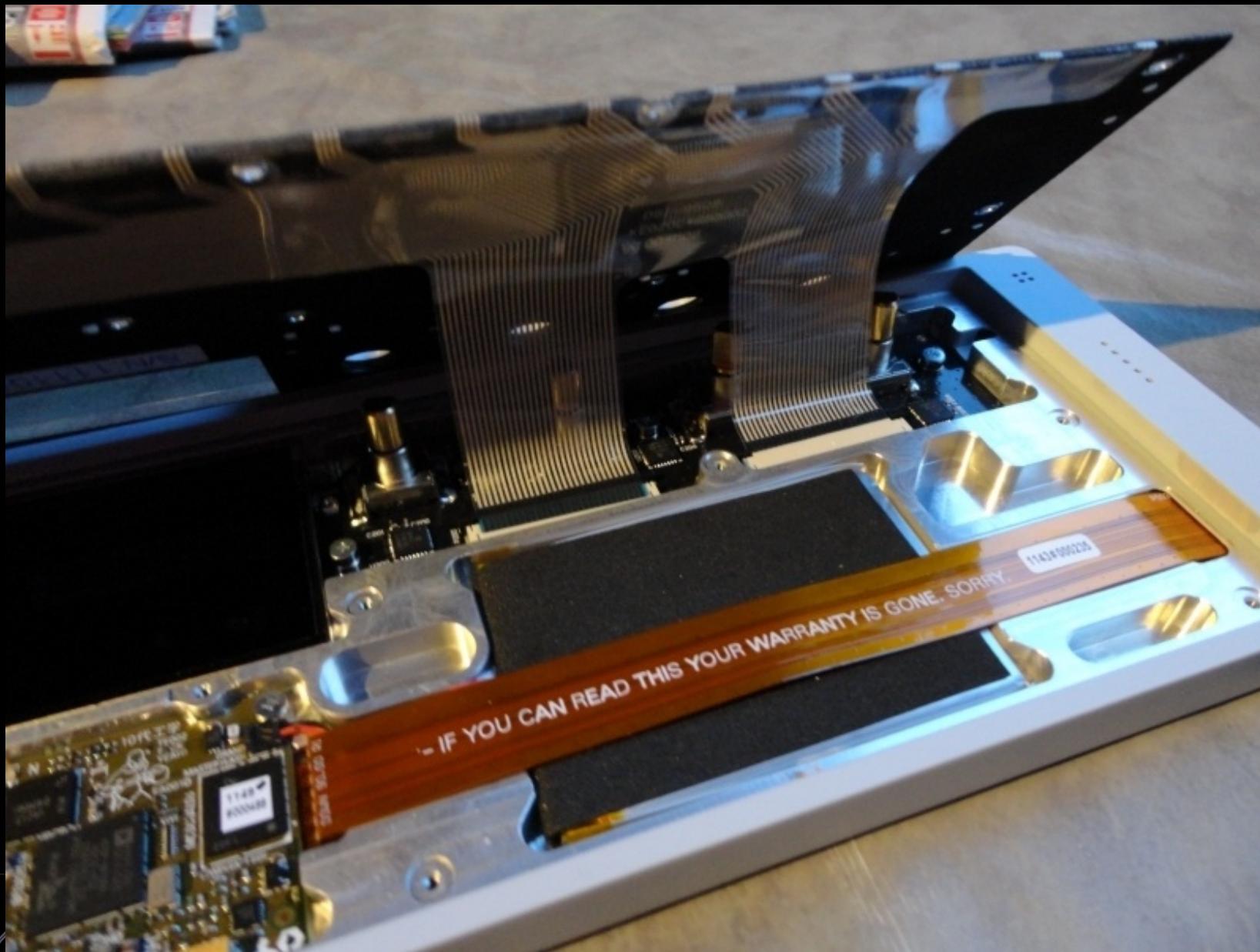
< 1 - 7 of 7 > Go to: 0

STEP2: GATHER MORE INTEL

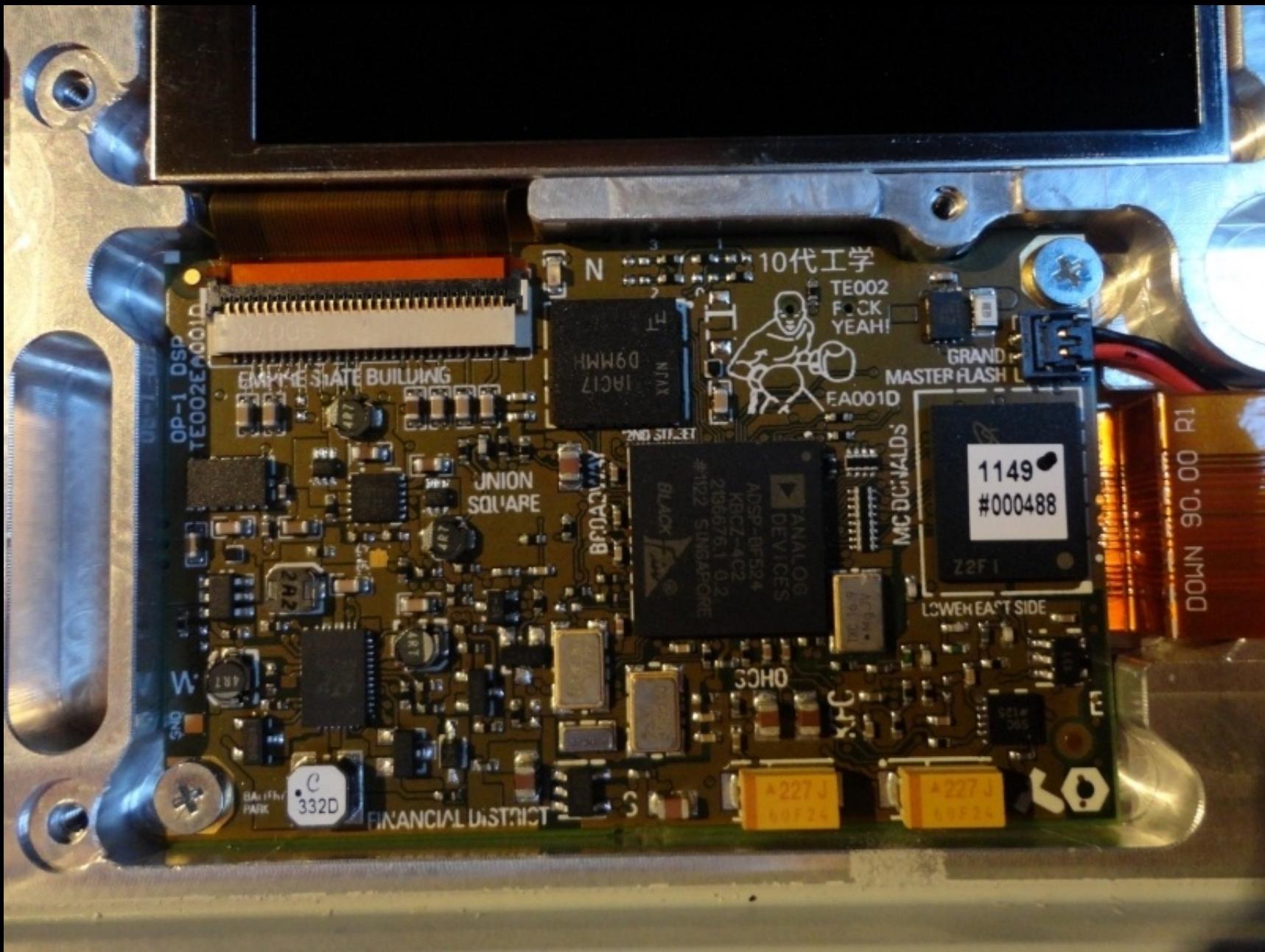
- Found beautiful pictures of the OP-1 PCBs
- CPU is Analog Devices BlackFin DSP (BF-524)



STEP2: GATHER MORE INTEL



STEP2: GATHER MORE INTEL



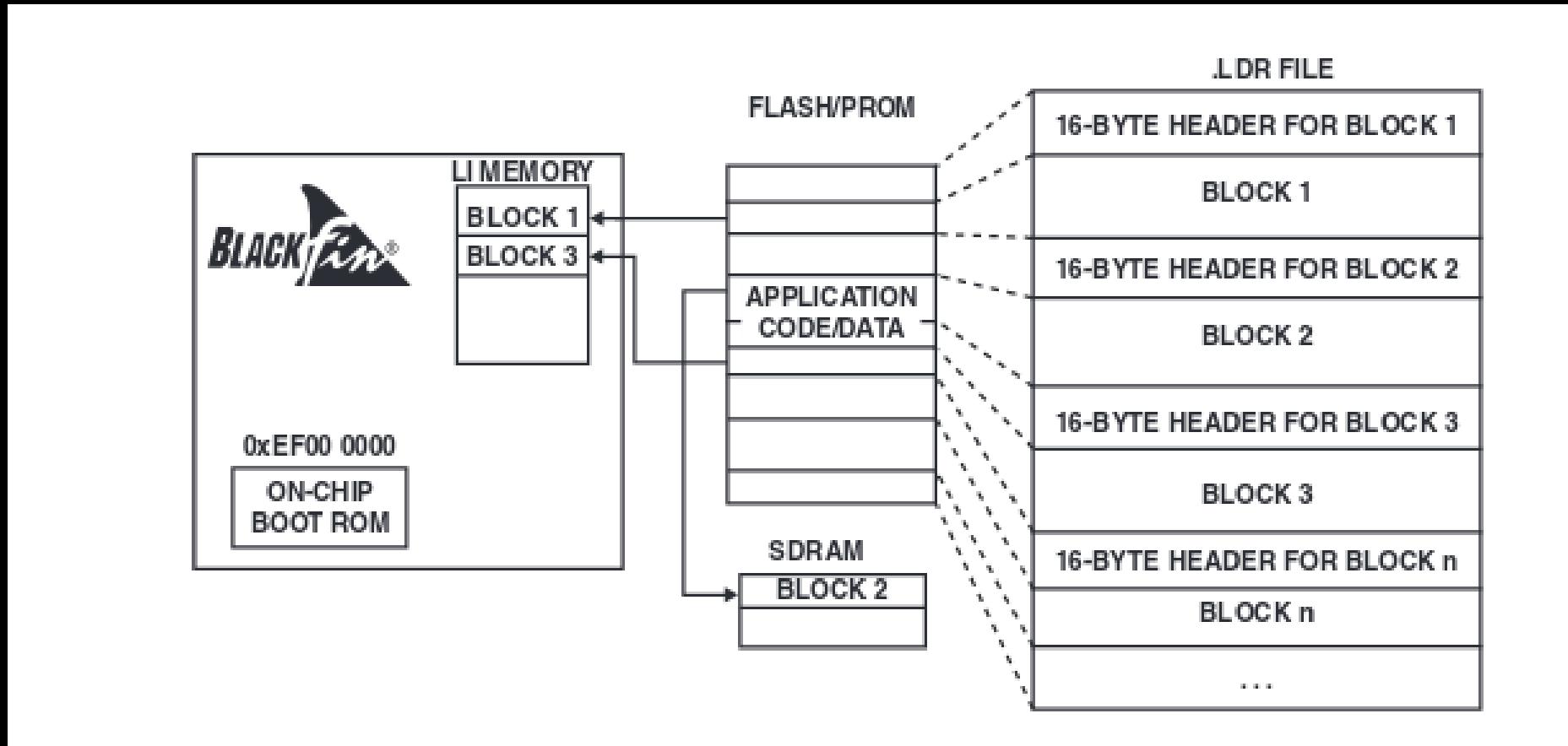
BlackFin DSPs

- 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/tabcascoeye/lxr2dxe>
- 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

File Compare | Copy Left | Copy Right | Delete | Same | New | Modified | Filters ▾

_op1_14203.op1.ed] _4.extracted

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/taba/Downloads/_op1_076.op1.extracted/_4.extracted

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	8.7 kB	Mo 21 Mär 2016 19:24:36
↳ delay.svg	10.5 kB	Mo 21 Mär 2016 19:24:36
↳ duallfo.svg	4.1 kB	Mo 21 Mär 2016 19:24:36
↳ iter.svg	13.5 kB	Mo 21 Mär 2016 19:24:36
↳ simple.svg	4.0 kB	Mo 21 Mär 2016 19:24:36
↳ slump.svg	21.6 kB	Mo 21 Mär 2016 19:24:36
↳ tempo.svg	36.9 kB	Di 22 Mär 2016 14:36:36
↳ op1.db	97.3 kB	Di 22 Mär 2016 08:56:50
↳ op1_factory.db	2.1 MB	Do 24 Mär 2016 10:40:20
↳ OP1_vdk.ldr	241.1 kB	Mo 21 Mär 2016 19:28:02
↳ te-boot.ldr		

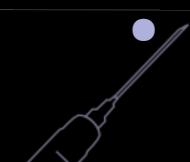
RWXX - X X - 34 months

STEP 3: GET MOTIVATION AND HELP

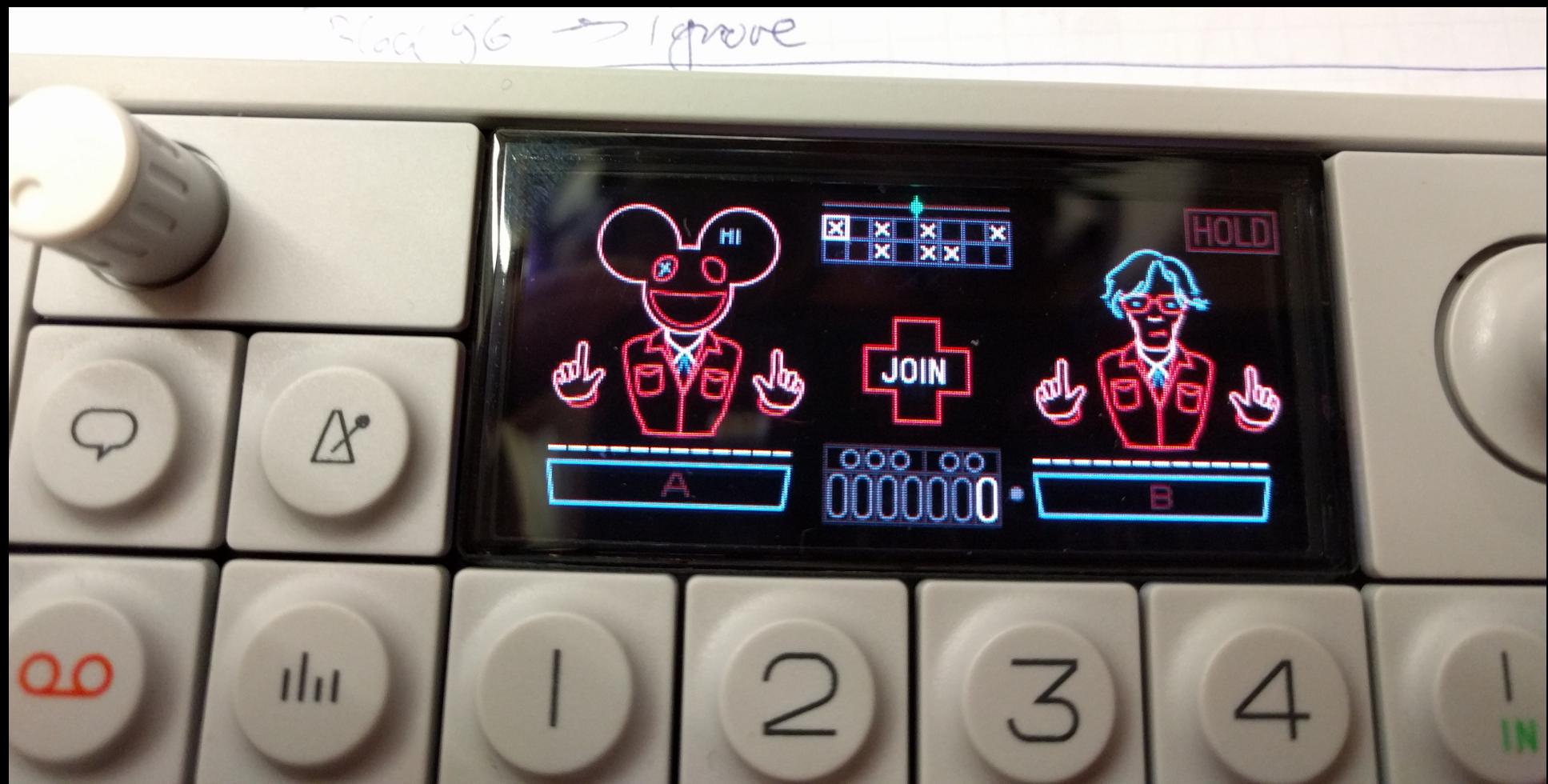


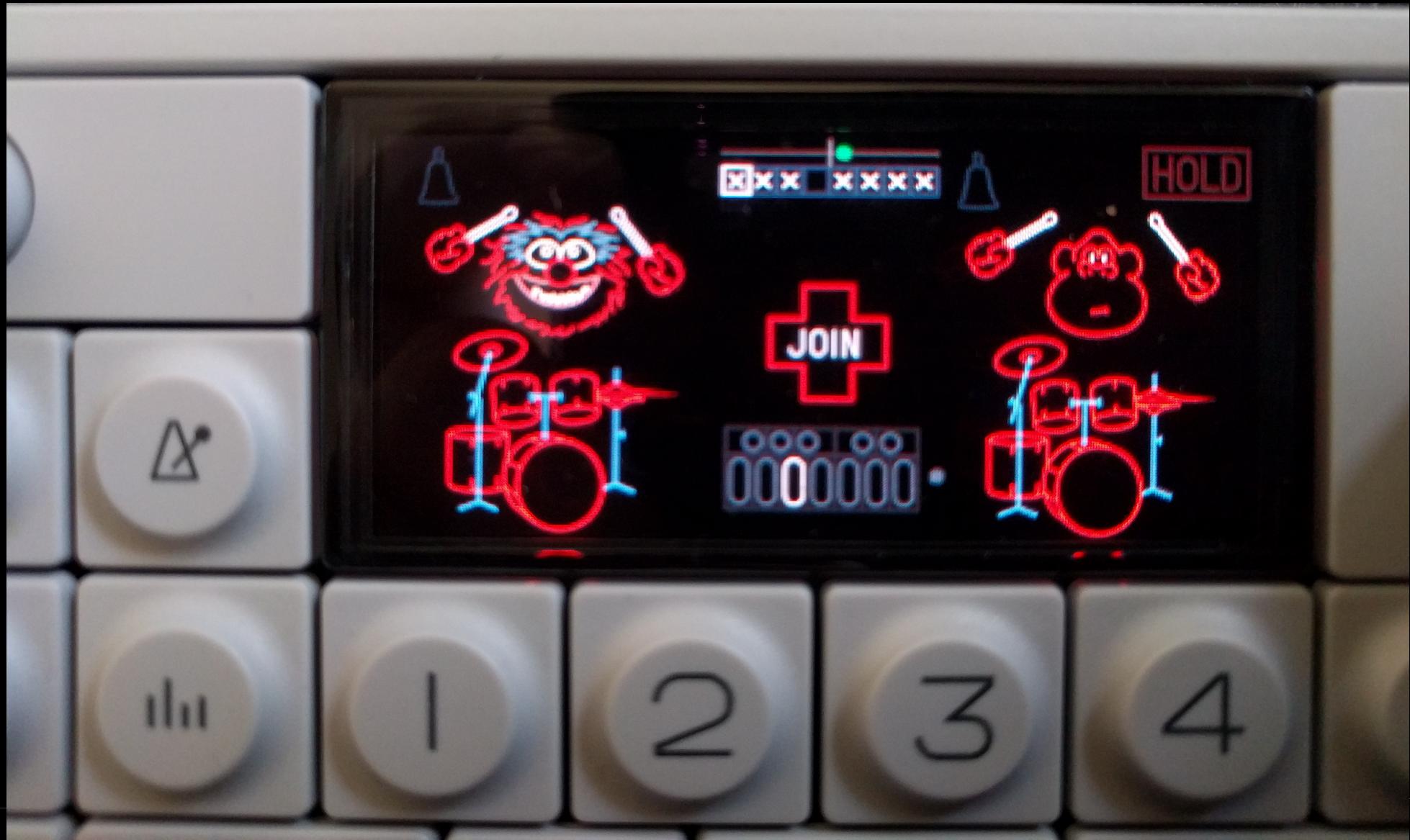
STEP 3: GET MOTIVATION AND HELP

- 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





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

71

X

||

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!)

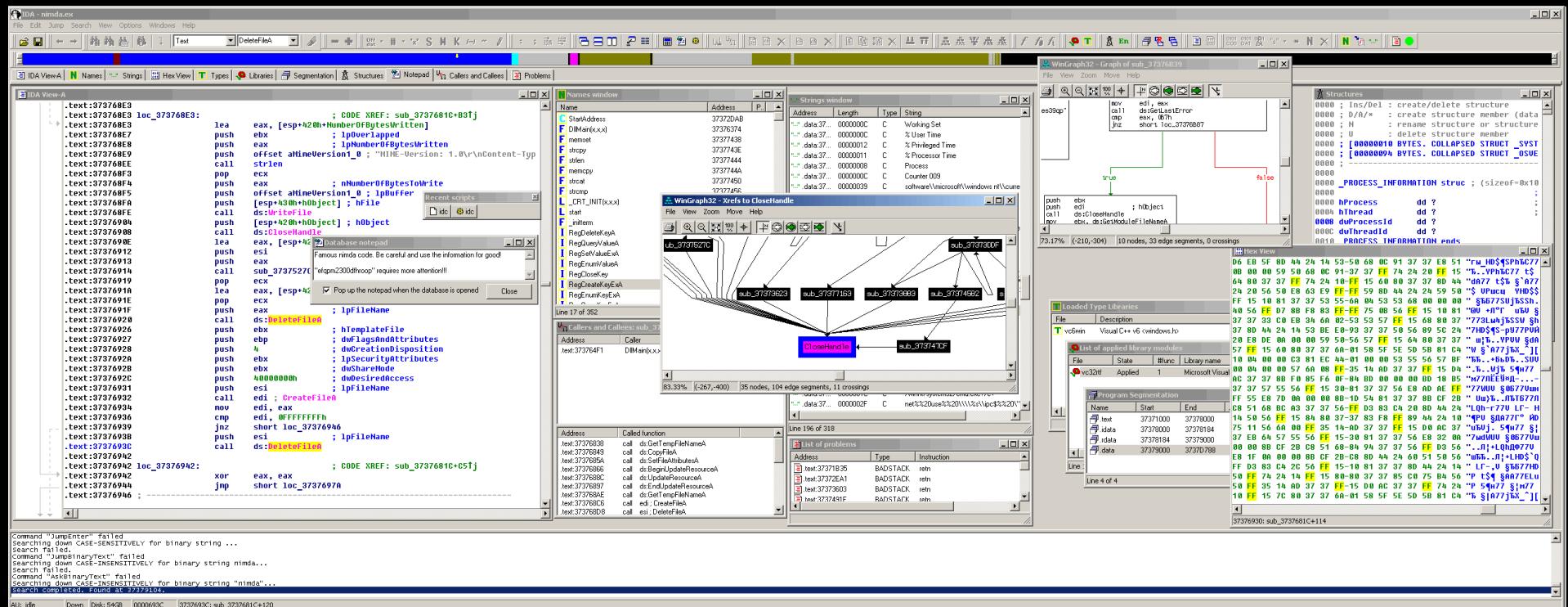
- And this:

From teenage engineering <support@teenage.engineering>★

Subject OP-1 custom firmware

To tabascoeye@gmail.com★

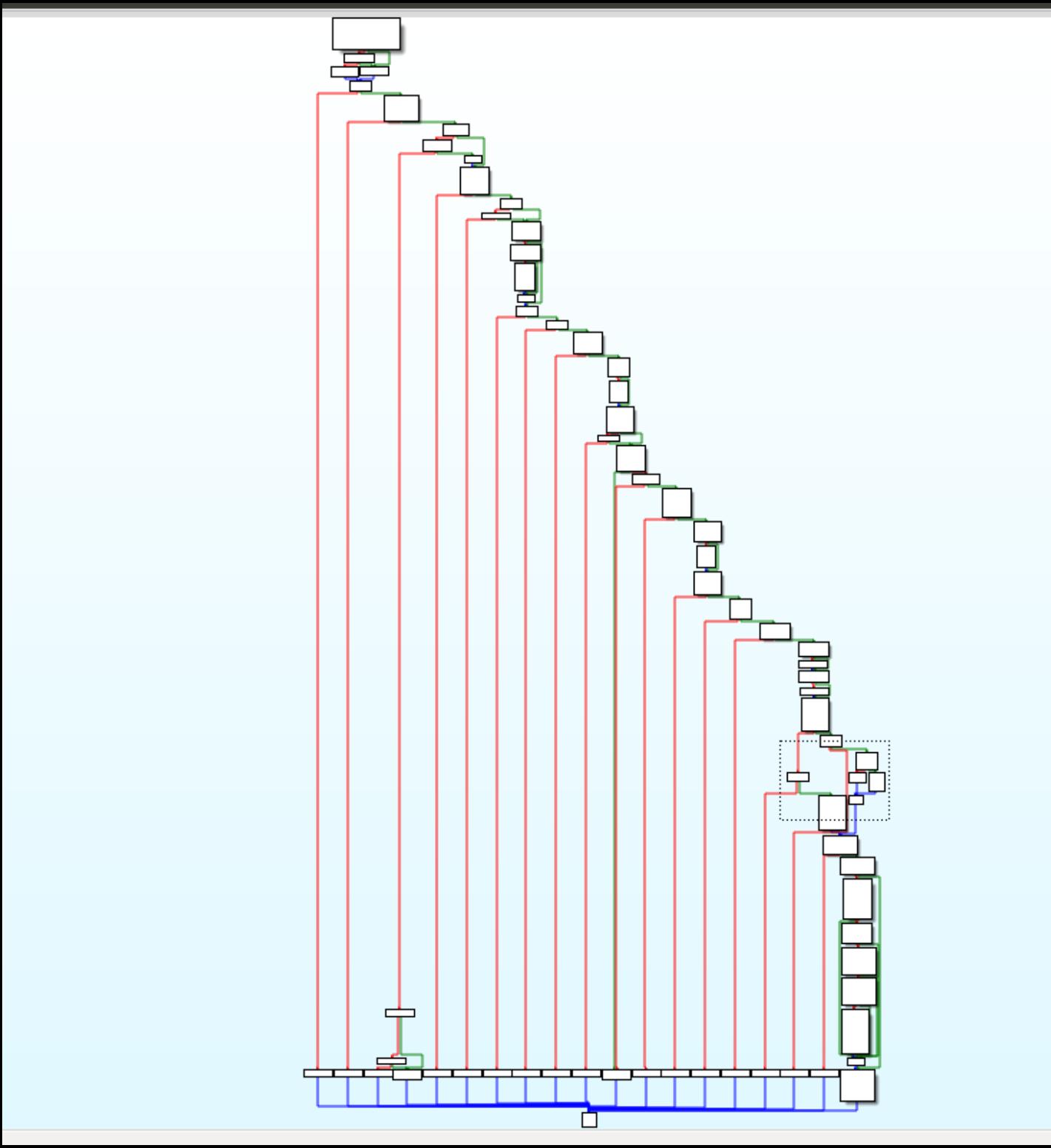
STEP4: GREETINGS, IDA



STEP4: GREETINGS, IDA

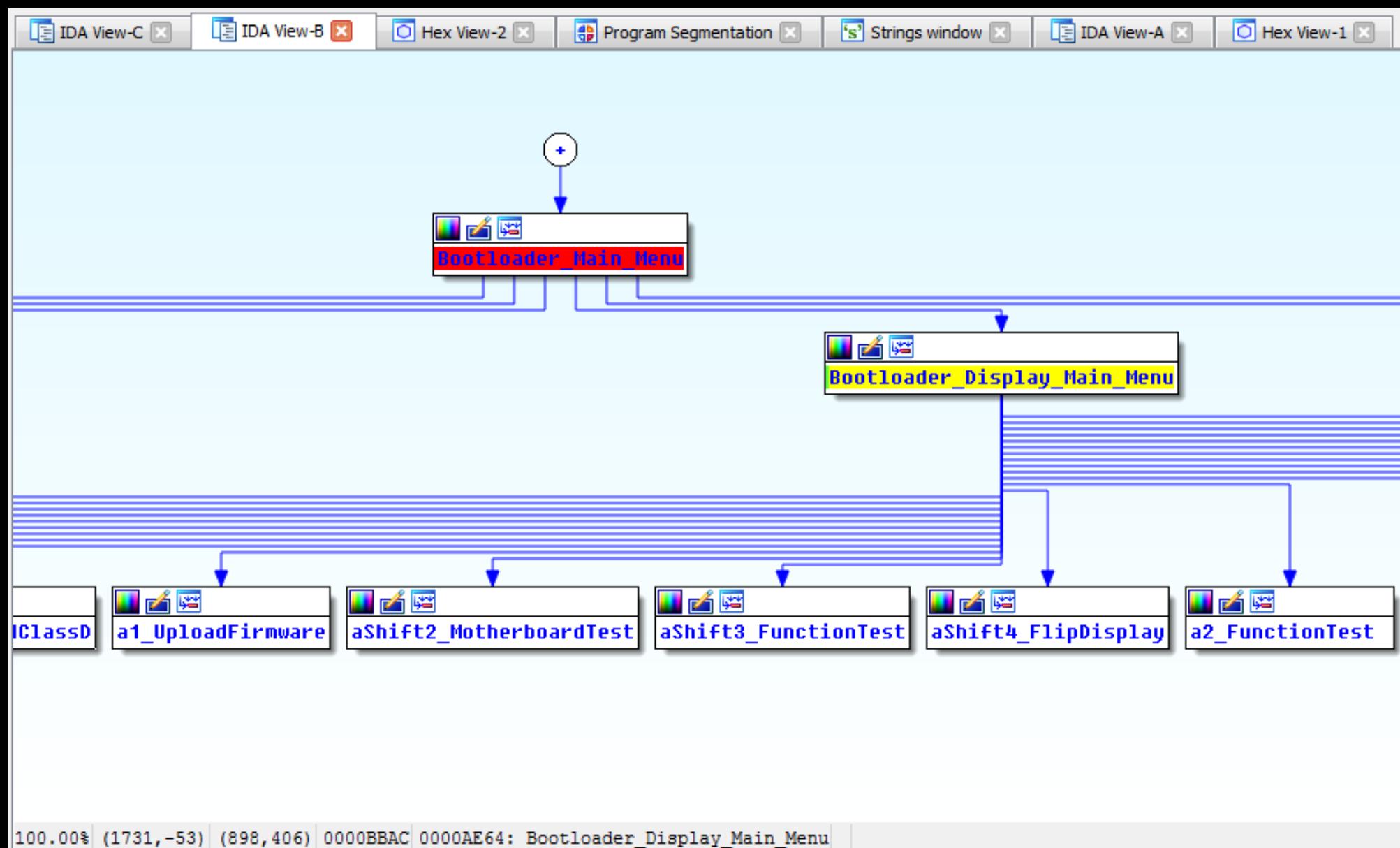
- pretty steep learning curve
- Especially with a custom processor plugin (i.e. no x86)

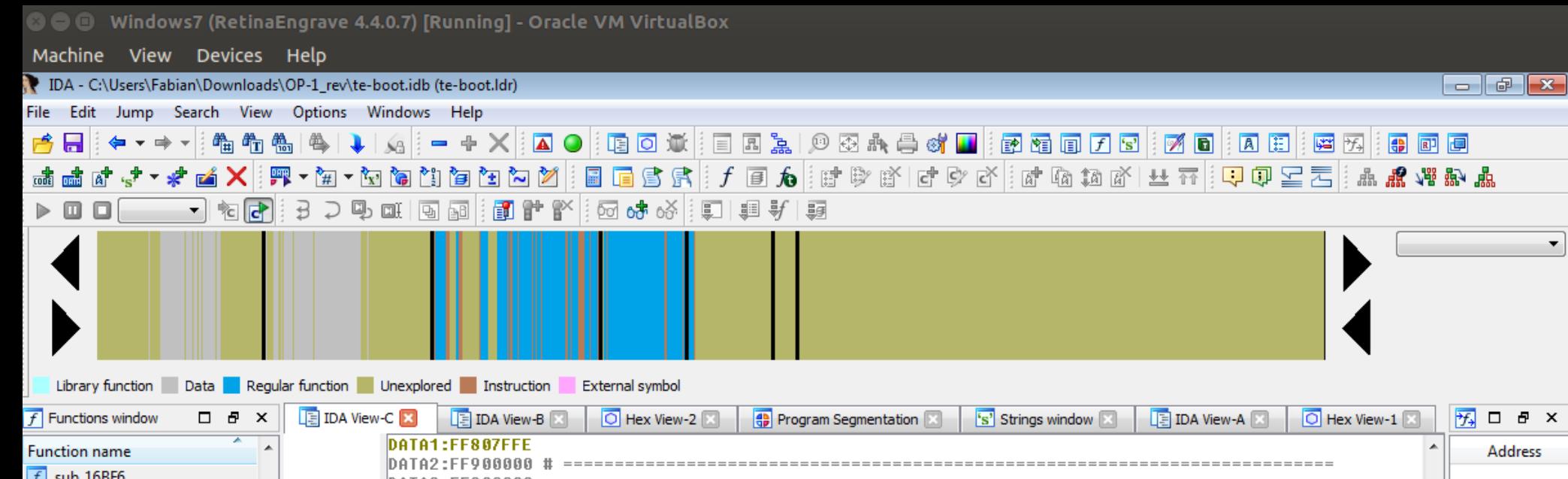




te-bootldr VS OP1_vdkldr

- 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.)





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

```
R0.L = 0x5dcc;          # R0=0xFF805dcc
R0.H = 0xFF80;           # R0=0xFF805dcc
                      -> a1_UploadFirmware -> "1. Upload Firmware"
CALL display_text;
P1.L = 0x2be9;           # P1=0xFF902be9
P1.H = 0xFF80;           # P1=0xFF802be9
                      -> unk_FF802BE9
R0 = B[P1] (2);
CC = (R0 == 0x0);
IF !CC JUMP loc_AF20;   # R0=0xFF805e30
```

```
;      # R0=0xFF805de0
;      # R0=0xFF805de0
-> aShift2_MotherboardTest -> "shift + 2. Motherboard test"
text;
;      # R0=0xFF805dFc
;      # R0=0xFF805dFc
-> aShift3_FunctionTest -> "shift + 3. Function test"
text;
;      # R0=0xFF805e18
;      # R0=0xFF805e18
-> aShift4_FlipDisplay -> "shift + 4. Flip Display"
text;
F3C;    # R0=0xFF805e44
```

```
loc_AF20:             # R0=0xFF805e30
R0.L = 0x5e30;
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;
```

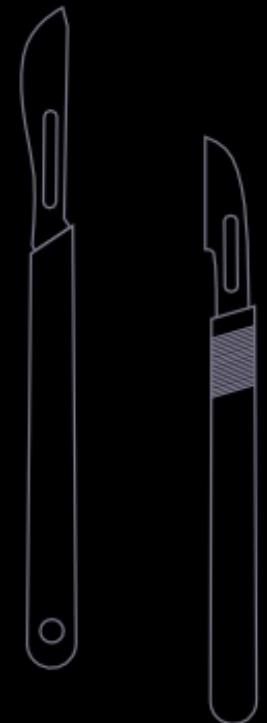
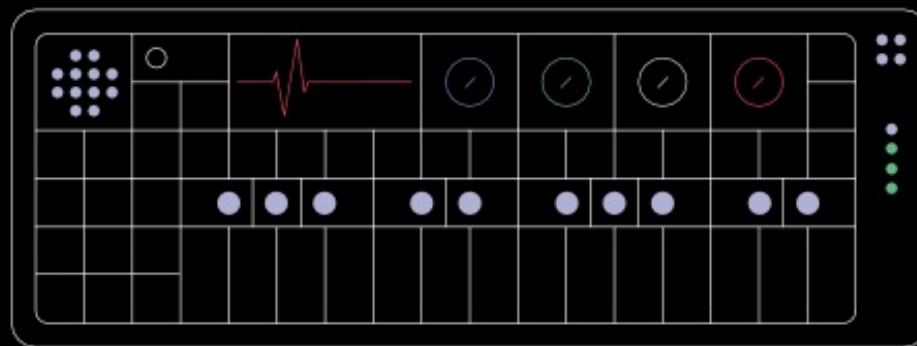
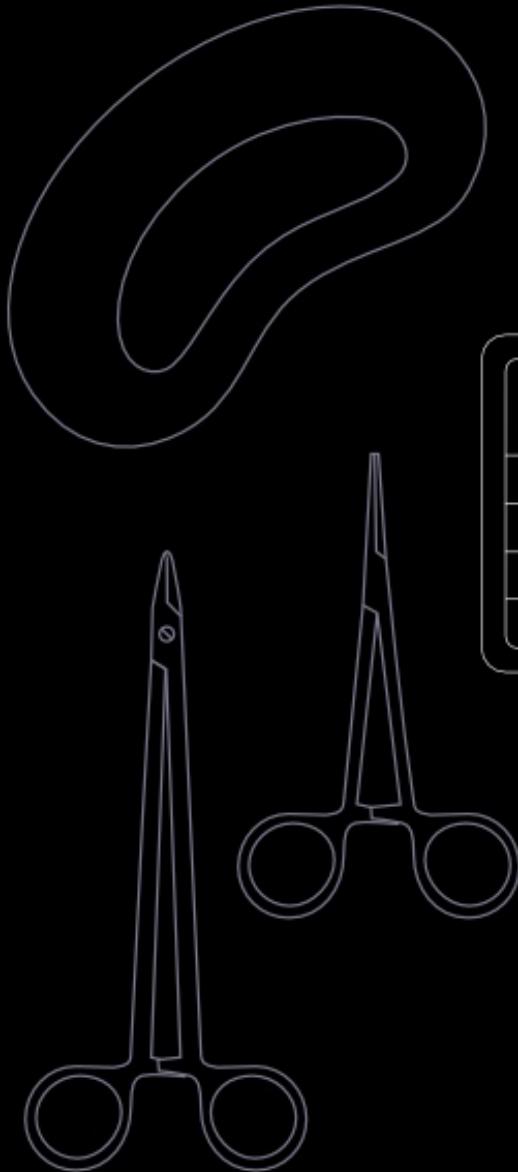
```
loc_AF3C:             # R0=0xFF805e44
R0.L = 0x5e44;
R0.H = 0xFF80;           # R0=0xFF805e44
                      -> a7.FactoryReset -> "7. Factory reset"
CALL display_text;
R0.L = 0x5e58;           # R0=0xFF805e58
R0.H = 0xFF80;           # R0=0xFF805e58
                      -> a8_FormatDrive -> "8. Format drive"
CALL display_text;
R0 = ROT R7 BY 0x0;
```

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

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 ipc, 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