

# Brute-Forcing Lockdown Harddrive PIN Codes

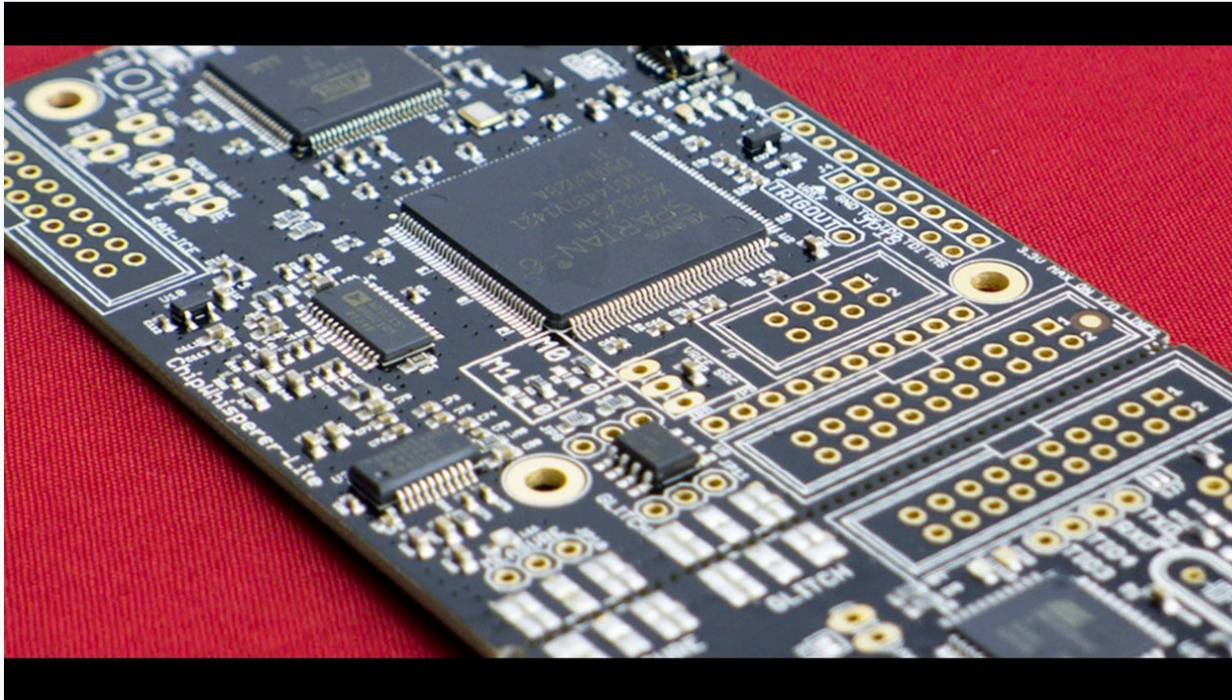


**Colin O'Flynn**



# ABOUT ME

## ChipWhisperer-Lite: A New Era of Hardware Security Research



Embedded security - is it an oxymoron? Learn the truth through a series of hands-on labs targeting computer and electrical engineers.

Created by

Colin O'Flynn



---

**331 backers** pledged \$88,535 CAD to help bring this project to life.

# TYPES OF SECURE DRIVES





# Previous Work

## Joffrey Czarny & Raphaël Rigo

Presentation at Hardware.io:

[http://hardware.io/wp-content/uploads/2015/10/Slide-hardware\\_re\\_for\\_software\\_reversers-By-Czarny-Rigo.pdf](http://hardware.io/wp-content/uploads/2015/10/Slide-hardware_re_for_software_reversers-By-Czarny-Rigo.pdf)


Lots of details in paper:

[https://www.sstic.org/media/SSTIC2015/SSTIC-actes/hardware\\_re\\_for\\_software\\_reversers/SSTIC2015-Article-hardware\\_re\\_for\\_software\\_reversers-czarny\\_rigo.pdf](https://www.sstic.org/media/SSTIC2015/SSTIC-actes/hardware_re_for_software_reversers/SSTIC2015-Article-hardware_re_for_software_reversers-czarny_rigo.pdf)

Me →  
Czarny & Rigo's Paper →

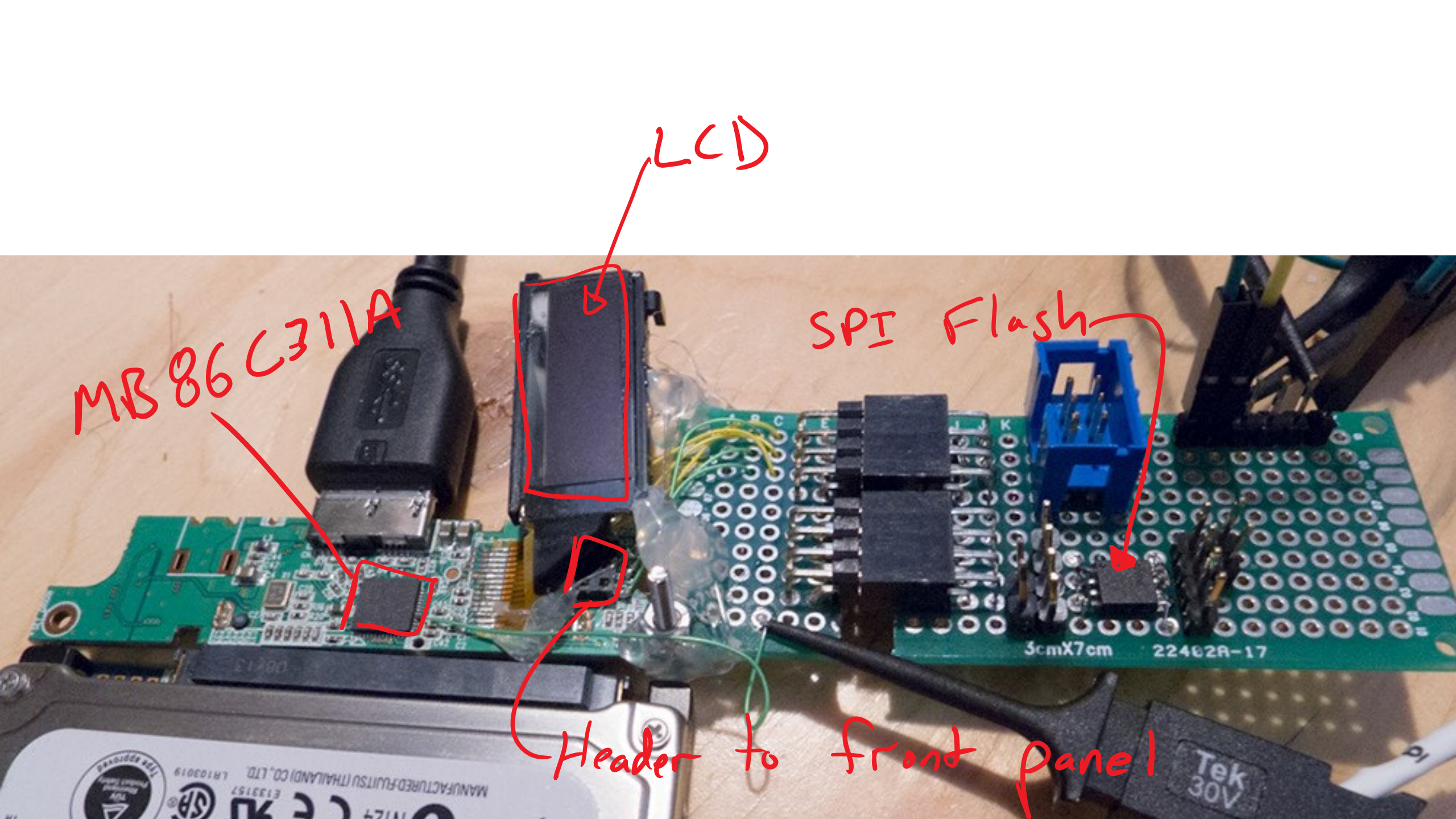






BRUTE  
FORCING





MB 86 C311A

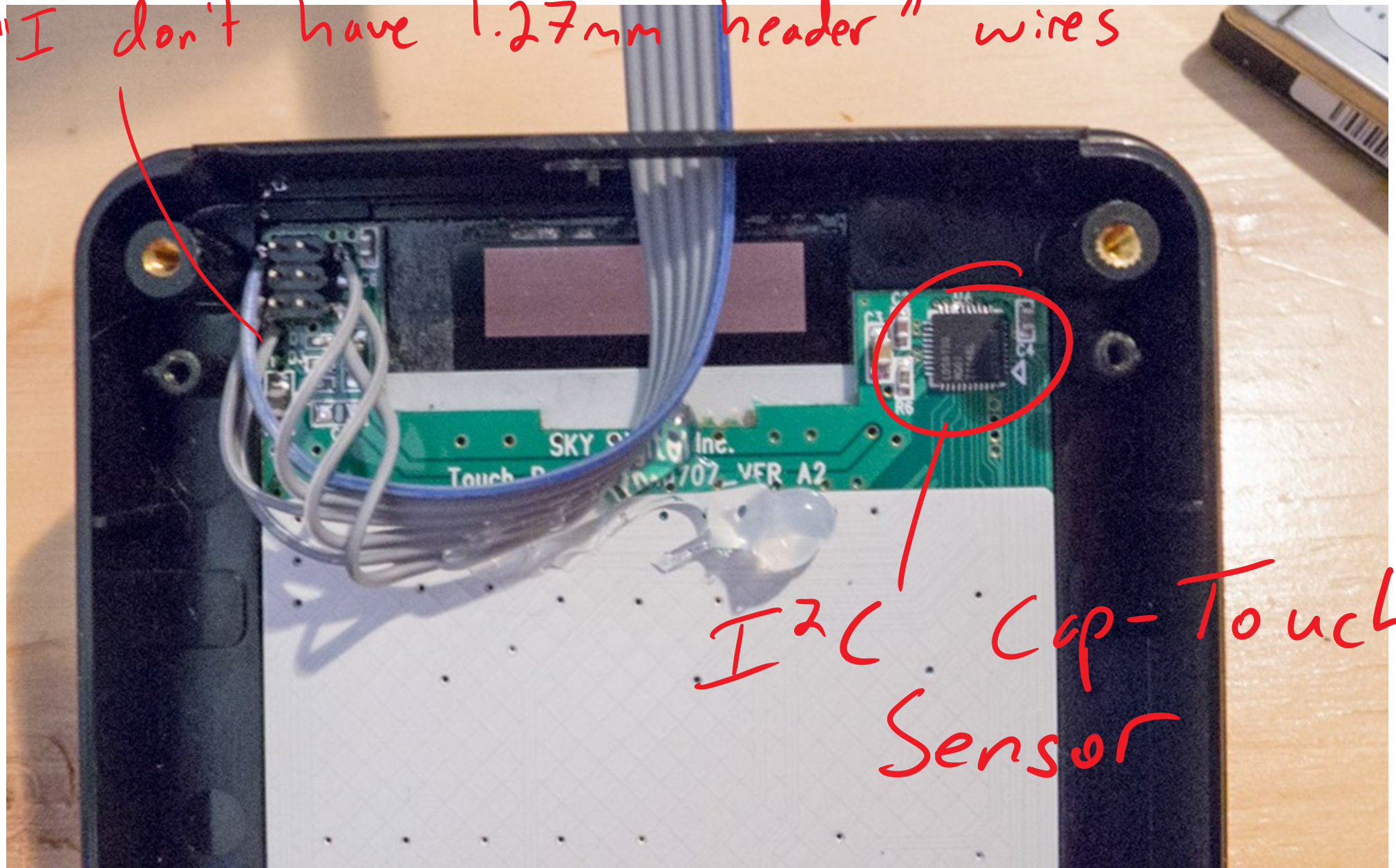
LCD

SPI Flash

Header to front panel

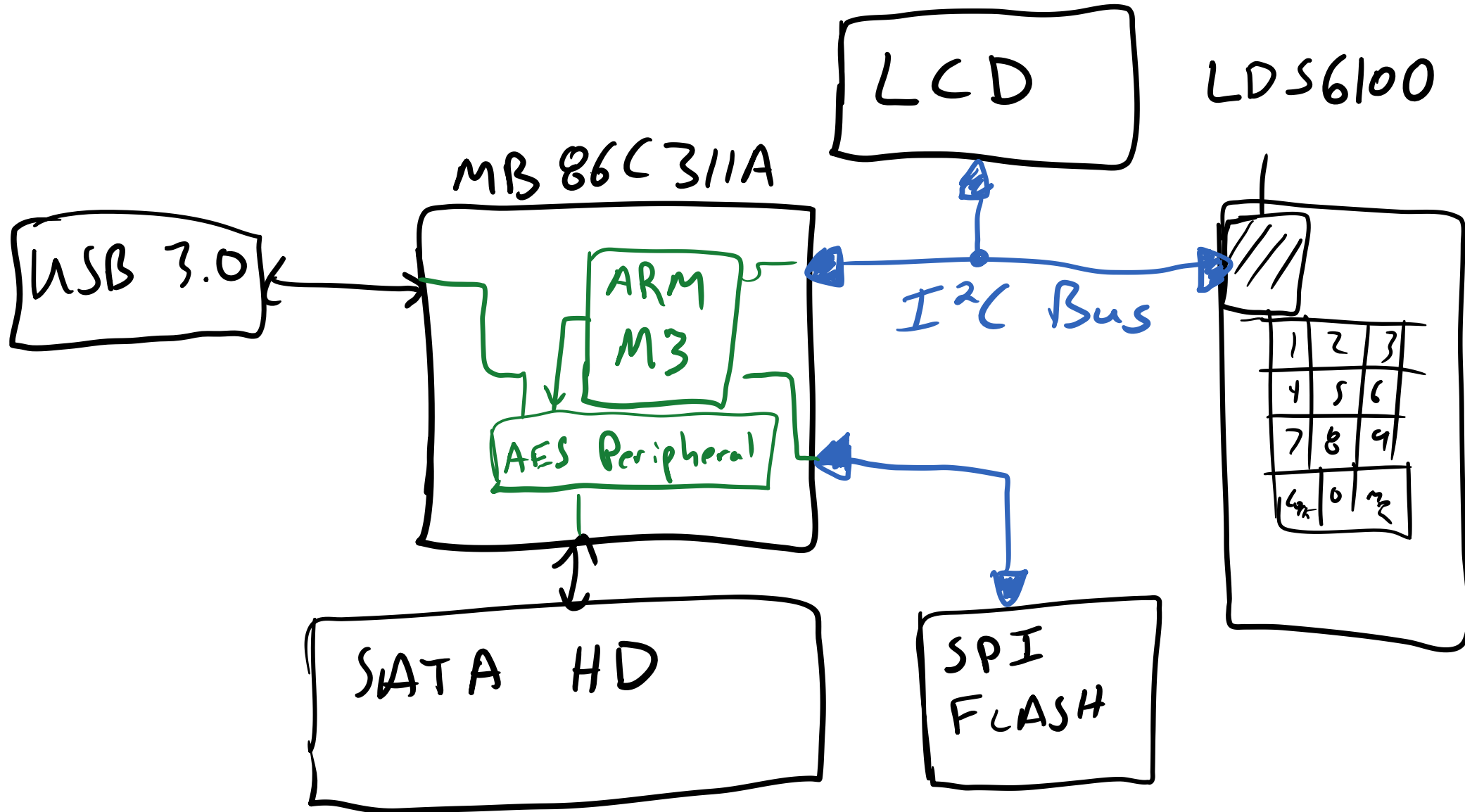


"I don't have 1.27mm header" wires



I2C Cap-Touch  
Sensor

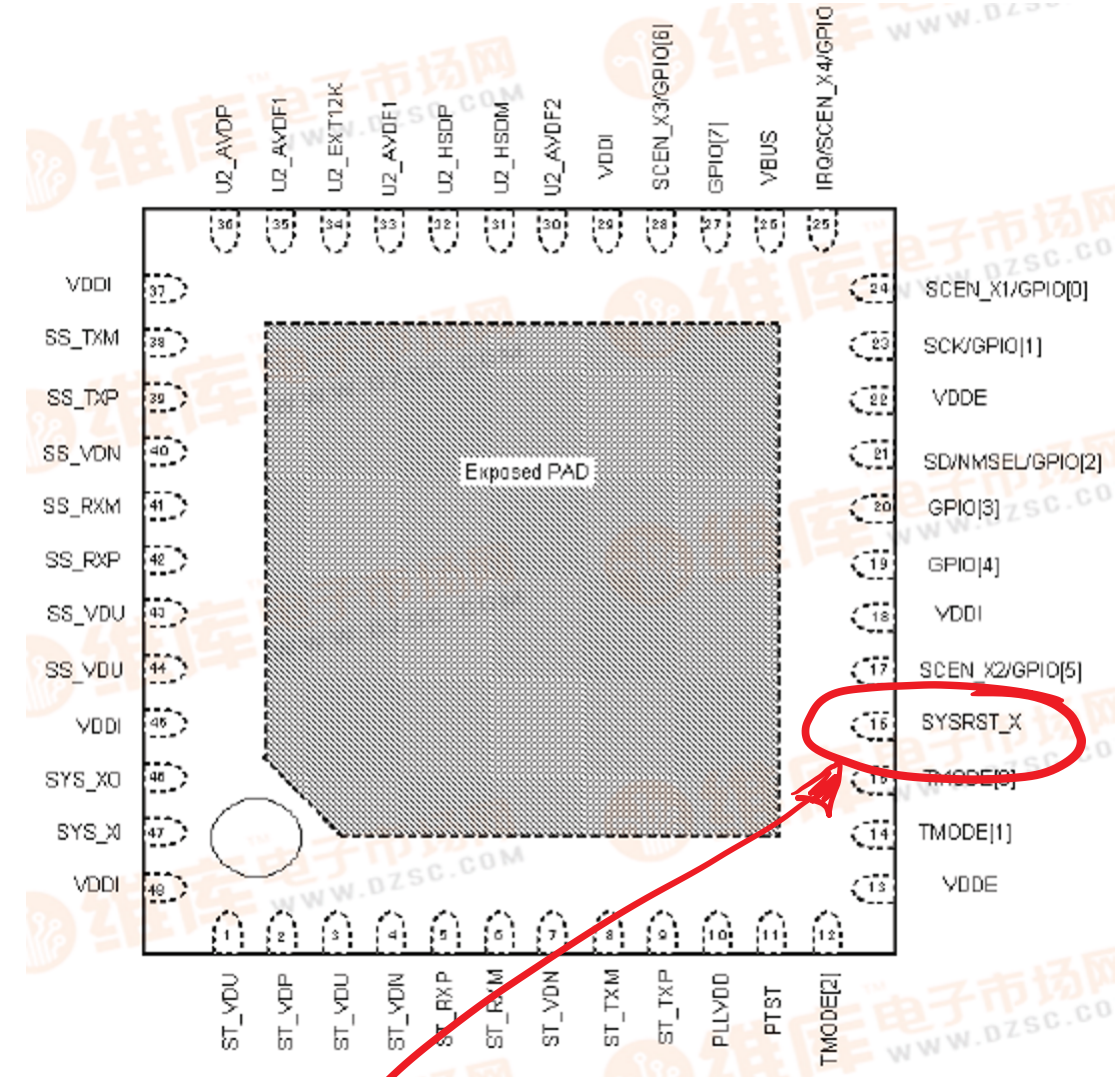
# Block Diagram





### 3. Turning on/off the power supply

item	Regulator		Pin
Turning on/ off the power supply	3.3V Power supply	Digital power supply for external IO	VDDE
		SATA 3.3V analog power supply	ST_VDP
		USB2.0 3.3V analog power supply	U2_AVDF1, U2_AVDB
Turning on/off the power supply	1.2V Power supply	Analog power supply for PLL	PLLVD
		Digital power supply for internal core	VDDI
		SATA 1.2V analog power supply	ST_VD, ST_VDU
		USB3.0 1.2V analog power supply	SS_VDN, SS_VDU
		USB2.0 1.2V analog power supply	U2_AVDF2, U2_AVDP

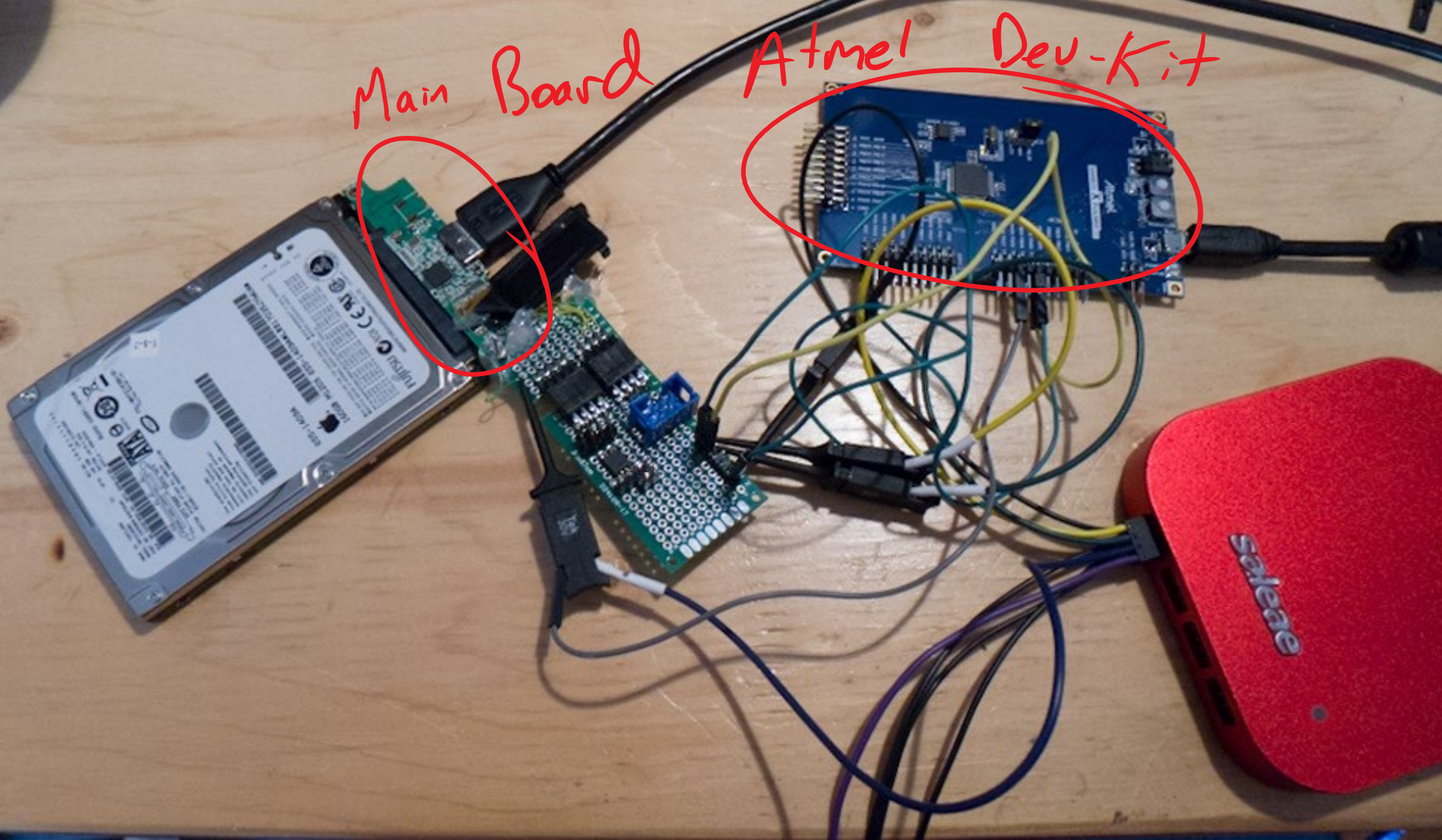


Can we bypass delay?



Main Board

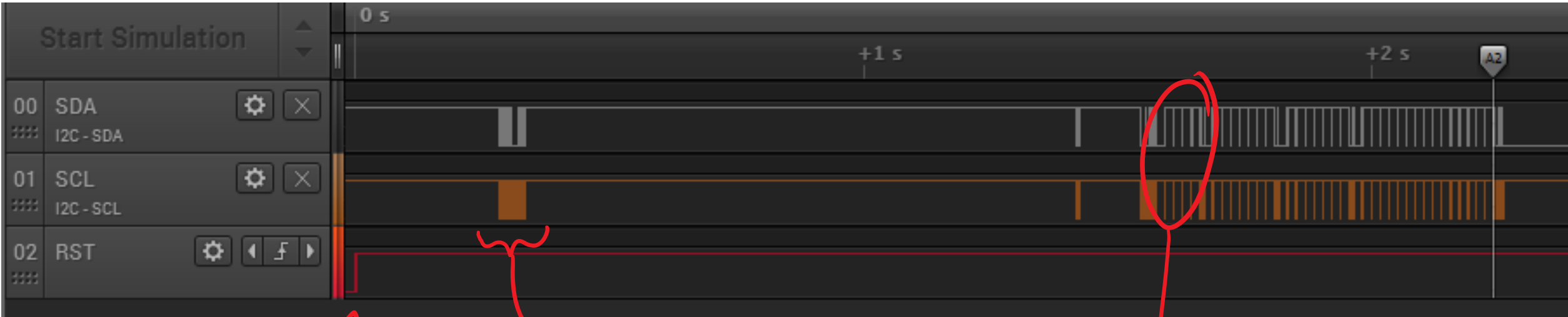
Atmel Dev-Kit





1. Wait for I<sup>2</sup>C poll
2. Feed in button presses.
3. Check response.

<https://github.com/colinoflynn/hddkeyboard-spoof-demo/>



Reset released

Initialization of LCD

Polling for buttons



# FINDINGS

1. Time-out not stored in NVM.  
↳ Can reset chip to bypass waits.
2. "Reasonable" entry speeds enforced  
↳  $\sim 0.5s$  for 4 digits
3. Boot involves about 1.5s delay.

# RESULTS

- 4 digit pin takes 2.23 s

PIN LENGTH	GUESS TIME (WORST CASE)
4	6.2 hrs
5	2.6 days
6	26 days
7	260 days





You purchased this item on Dec 23 2015.

[View this order](#)



## Satechi LockDown USB 3.0 Super-Speed 256-bit Encrypted Portable External 2.5" SATA Hard Drive Enclosure

by [Satechi](#)



13 customer reviews

**Currently unavailable.**

We don't know when or if this item will be back in stock.

- Quality OLED screen enables easy password input, menu navigation, HDD info and more
- Incorporates capacitance touch panel numeric keypad - Unlock the drive with your own unique 4 to 8 digit password
- USB 3.0 Super-Speed (5Gbps) driver also supports USB 2.0, ARM based 32bit Controller
- Measures (W) 3.1 x (H) 5 x (D) 0.5 inches / 3.25 ounces (w/o HDD)



**EARN A \$5 CREDIT FOR  
EACH FRIEND WHO JOINS** [Refer a friend](#)



CHECKING  
CHIPS



OK! How SECURE ARE THESE?

Previous work by Czarny & Rigo:

## 8 Conclusion

Starting with no information, we managed, in full black box, to have a good understanding of the way this encrypted drive enclosure works.

While we know the crypto design is a fail, because all the encryption related data is stored on the drive itself, with no enclosure dependent secret, we were unable to actually exploit it.



# SWAP IC FOR VIRGIN

→ Device worked.

↳ NO fuse bits  
or other secret  
specific to  
manufacture.



## Compare Bins

Two versions  
of program  
for Zalman  
drive.

(This is from  
Czarny & Rigo)

```

zalman\fw\UE400_firmware_1-37(FAT).bin
0000 0000: 32 FF 1F 81 8E F2 DE E2 34 76 A0 2B 77 CC 03 E3 2  .iiA=i0 4uA+u! .0
0000 0010: 92 A9 6E 62 37 E5 8E 48 EA 5D 58 97 8D 5E A5 E6 #0nb70AH 0 IXu1\Nu
0000 0020: 84 2E 01 00 42 00 00 00 AA C8 01 A7 67 D6 C1 18 3. . . . . 1L. 2g f 1.
0000 0030: B0 4D 92 1B 28 0C 38 8F AB D1 0E 18 68 5C 21 D1 MfE. C. 88 2D. . h\!D
0000 0040: EC F8 0B D7 6D CB 4F 13 05 8A C3 32 F7 6E 21 38 g. . i m 0. . e 2. n!8
0000 0050: 2A C1 36 9E 5A 1C 6B BF 78 F2 EC BC 7B 5F A1 6C *+6xZ. kJ x= g!k _1l
0000 0060: 2C A4 5A B1 6F 1B 80 E2 53 7E A4 FC FA 67 00 18 nZ . . . . . 0^n 3+g. .
0000 0070: 50 63 63 D0 83 D1 E3 9A F5 D6 16 88 C2 19 67 F1 Pcc0a00i . . i . e6. g±
0000 0080: A8 77 7F A4 C1 76 3D A9 4C 6C 0B 76 1E 3E 18 BA 2w0n L u =0 1L. v. > . ||
0000 0090: 67 F2 42 55 FC C0 91 A8 10 83 E1 7B DF E6 26 E0 g= BU 3 Læi . . âB< µ&0
0000 00A0: 33 44 4B 90 50 A3 55 32 7C 39 12 0A 89 19 DF E0 3DKE PûU2 19. . . S. °ó
0000 00B0: F2 00 30 07 CB AC EC EA B1 E9 DA 9C G6 02 0E 55 =. 0. 2qyú 0ú r f. . U
0000 00C0: 14 CC 19 19 6D 31 85 41 A7 3F 92 15 9F F2 CA 77 . J. . n1aA 2?fE. f= 2w
0000 00D0: 90 D0 BF 77 63 E8 0A 85 88 14 2E 49 3E 22 F5 05 E0 1w0p. . . e. . I>'S.
0000 00E0: 96 B0 C1 3A 93 23 4C 51 7C 7A BB CD C3 19 10 7F ü1=:#LQ izn=|. . 0
0000 00F0: B2 8F 34 59 B7 0E B4 F2 75 43 10 D5 5B 22 7D 86 84YA. |= uC. 2 ['>â
0000 0100: 0E 93 D1 03 43 37 BB D1 1C C9 DF 95 EC 7C 73 37 . 0D. C7nD . r 0 0y!s?
0000 0110: 83 90 A9 EF 89 A1 2B 12 BB 52 38 C2 0B 66 8F DC æ0' 'e i+ . rR8 T. fâ
0000 0120: C5 3C 47 D6 9B 97 4F F1 3A 01 87 DC C6 50 18 95 <Gí0u0± . . :. ç. âP. 0
0000 0130: D7 0E 75 E0 17 83 32 A0 19 3D 46 5A DC 44 88 DF î. u0. â2â . =FZ. Dê
0000 0140: E4 D0 84 89 86 FC 9B BD FA D7 F1 BE C5 79 EF C4 0âæââ°0ç . î±¥+y'
0000 0150: 96 2D D2 5C 5C F4 4C E8 24 83 93 CB 12 B1 18 04 ü-E-\\MLB $â0 . . .
0000 0160: 94 BD 16 44 49 C3 54 36 76 A6 4A D1 5D 4C BE E0 0ç. DI T6 uâJ0 JL#0
0000 0170: FF 60 7D 96 D3 DD 9C C7 9A 69 C0 60 C7 7F EB 8F 'üE! fâ ü i L' . â0u8
0000 0180: DE F1 0E CB 7F C9 55 28 D7 23 7E 1F 98 10 00 4D î±. 00rJ< î#~. y. . M
0000 0190: 53 8D CF 14 50 32 6C 6E 82 C6 E1 06 2B C6 22 B4 $ix. P2ln éâB. +â' |
0000 01A0: 8A 23 ED EB F4 46 0F 15 02 EF 45 0A 77 59 A3 9B è#YúYMF. . 'E. wYú0
0000 01B0: 21 54 1F 5B DD 68 6D 07 F3 A3 77 AD 73 99 8E 70 !T. [ ihm. 2úwi s0âp

zalman\fw\UE400_firmware_1-37(NTFS).bin
0000 0000: 01 ED 10 47 A0 70 D3 BE A4 B0 6B DE 49 0E 09 67 . Y. GâPEY 0úki L. . g
0000 0010: E1 87 DB B4 37 87 4B 5A 4B 6D 28 F0 9E 88 21 CD 0ç 7çKZ km<-xê! =
0000 0020: 94 2E 01 00 02 00 00 00 AA C8 01 A7 67 D6 C1 18 0. . . . . 1L. 2g f 1.
0000 0030: CC 4D 92 1B 54 0C 38 8F D7 D1 0E 18 14 5C 21 D1 MfE. T. 88 îD. . . \!D
0000 0040: 90 F8 0B D7 6D CB 4F 13 05 8A C3 32 F7 6E 21 38 E. . i m 0. . e 2. n!8
0000 0050: 2A C1 36 9E 26 1C 6B BF 04 F2 EC BC 7B 5F A1 6C *+6x&. kJ x= g!k _1l
0000 0060: 50 A4 5A B1 13 1B 80 E2 4F 7E A4 FC F6 67 00 18 PnZ . . . . . 0^n 3+g. .
0000 0070: 4C 63 63 D0 83 D1 E3 9A F9 D6 16 88 36 1A 67 F1 Lcc0a00i . . i . e6. g±
0000 0080: BC 77 7F A4 3C 75 3D A9 B0 6F 0B 76 EA 3D 18 BA 2w0n L u =0 10. v0 =. ||
0000 0090: 6B F2 42 55 EB C0 91 A8 6C 83 E1 7B A3 E6 26 E0 k= BU 3 Læi 1âB< µ&0
0000 00A0: 27 44 4B 90 2C A3 55 32 00 39 12 0A F5 19 DF E0 'DKÉ. úU2 . 9. . S. °ó
0000 00B0: 8E 00 30 07 A7 AC EC EA A5 E9 DA 9C B0 02 0E 55 2. 0. 2qyú 0ú r f. . U
0000 00C0: 00 CC 19 19 71 31 85 41 B3 3F 92 15 9F F2 CA 77 . J. . q1aA 1?fE. f= 2w
0000 00D0: EC D0 BF 77 6F E8 0A 85 88 14 2E 49 3E 22 F5 05 E0 1w0p. . . e. . I>'S.
0000 00E0: 96 B0 C1 3A 93 23 4C 51 7C 7A BB CD C3 19 10 7F ü1=:#LQ izn=|. . 0
0000 00F0: B2 8F 34 59 B7 0E B4 F2 75 43 10 D5 5B 22 7D 86 84YA. |= uC. 2 ['>â
0000 0100: 0E 93 D1 03 43 37 BB D1 1C C9 DF 95 EC 7C 73 37 . 0D. C7nD . r 0 0y!s?
0000 0110: 83 90 A9 EF 89 A1 2B 12 BB 52 38 C2 67 66 8F DC æ0' 'e i+ . rR8 T. fâ
0000 0120: 29 3C 47 D6 9B 97 4F F1 3A 01 87 DC C6 50 18 95 <Gí0u0± . . :. ç. âP. 0
0000 0130: D7 0E 75 E0 17 83 32 A0 19 3D 46 5A DC 44 88 DF î. u0. â2â . =FZ. Dê
0000 0140: E4 D0 84 89 86 FC 9B BD FA D7 F1 BE C5 79 EF C4 0âæââ°0ç . î±¥+y'
0000 0150: 96 2D D2 5C 5C F4 4C E8 24 83 93 CB 12 B1 18 04 ü-E-\\MLB $â0 . . .
0000 0160: 94 BD 16 44 49 C3 54 36 76 A6 4A D1 5D 4C BE E0 0ç. DI T6 uâJ0 JL#0
0000 0170: FF 60 7D 96 D3 DD 9C C7 9A 69 C0 60 C7 7F EB 8F 'üE! fâ ü i L' . â0u8
0000 0180: DE F1 0E CB 7F C9 55 28 D7 23 7E 1F 98 10 00 4D î±. 00rJ< î#~. y. . M
0000 0190: 53 8D CF 14 50 32 6C 6E 82 C6 E1 06 2B C6 22 B4 $ix. P2ln éâB. +â' |
0000 01A0: 8A 23 ED EB F4 46 0F 15 02 EF 45 0A 77 59 A3 9B è#YúYMF. . 'E. wYú0
0000 01B0: 21 54 1F 5B DD 68 6D 07 F3 A3 77 AD 79 99 8E 70 !T. [ ihm. 2úwi y0âp

```

# STREAM

# CIPHER

Keystream : E7 1A F1 37

$\oplus$

$\oplus$

$\oplus$

$\oplus$

Plain text : 2C 1F 09 1A . . .

Cipher text : CB 05 F8 2D



# Compare Bins

File Length

Flag?

Code

No difference in encrypted data

⇒ No diff in source at that byte.

zalman\fw\UE400_firmware_1-37(FAT).bin																													
0000	0000:	32	FF	1F	81	8E	F2	DE	E2	34	76	A0	2B	77	CC	03	E3	2	..üâ=i6	4vA+u!..0									
0000	0010:	92	09	5E	62	27	EE	9E	40	EA	5D	58	97	8D	5E	A5	E6	æ0nb70âH	0 IXu!~Nu										
0000	0020:	84	2E	01	00	42	00	00	00	7A	C8	01	A7	67	D6	C1	18	ä...B...	~L..egí±.										
0000	0030:	60	4D	92	1B	78	0C	38	8F	AB	D1	0E	18	68	5C	21	D1	ME.<.8â	7D...h~!D										
0000	0040:	EC	F8	0B	D7	3D	CF	4F	13	05	8A	C3	32	F7	6E	21	38	g°.îm~0.	..è 2.n!8										
0000	0050:	2A	C1	36	9E	5A	1C	6B	BF	78	F2	EC	BC	7B	5F	A1	6C	*+6xZ.kj	x=ýlç_í1										
0000	0060:	2C	A4	5A	B1	6F	1B	80	E2	53	7E	A4	FC	FA	67	00	18	ñZ...Ç0	S~ñ³.g..										
0000	0070:	50	63	63	D0	83	D1	E3	9A	F5	D6	16	88	C2	19	67	F1	Pccðâð0ü	Si.êr.g±										
0000	0080:	A8	77	7F	A4	21	76	3D	A9	40	6C	0B	76	1E	3E	19	BA	2wðñ~u=0	L1.v.>.										
0000	0090:	67	F2	42	55	FC	C0	91	A8	10	83	E1	7B	DF	E6	26	E0	g=BU³Læi	.âB<úµ&ó										
0000	00A0:	33	44	4B	90	50	A3	55	32	7C	39	12	0A	89	19	DF	E0	3DKéPúU2	!9...S..ó										
0000	00B0:	F2	00	30	07	CB	AC	EC	EA	B1	E9	DA	9C	C6	02	0E	55	=.0..²¼ýü	ñú rE..U										
0000	00C0:	14	CC	19	19	6D	31	85	21	A7	3F	92	15	9F	F2	CA	77	.J..m1âa	²?æ.f=µv										
0000	00D0:	90	D0	BF	77	63	E8	0A	85	88	14	2E	49	3E	22	F5	05	Eð~wcb.à	ê...I>"S.										
0000	00E0:	96	B0	C1	3A	93	23	4C	51	7C	7A	BB	CD	C3	19	10	7F	û~L:0#LQ	!zñ= ..â										
0000	00F0:	B2	8F	34	59	B7	0E	B4	F2	75	43	10	D5	5B	22	7D	86	4Yâ.. =	uC.²[">â										
0000	0100:	0E	93	D1	03	43	37	BB	D1	1C	C9	DF	95	EC	7C	73	37	.ðD.C7ñD	.r~ðý!s?										
0000	0110:	83	90	A9	EF	89	A1	2B	12	BB	52	38	C2	0B	66	8F	1C	âé0'ëí+	ñR8T.fâ										
0000	0120:	C5	3C	47	D6	9B	97	4F	F1	3A	01	87	DC	C6	50	18	95	<Gí0u0±	..ç..âP..ð										
0000	0130:	D7	0E	75	E0	17	83	32	A0	19	3D	46	5A	DC	44	88	DF	î.uó..â2â	..=FZ..Dê										
0000	0140:	E4	D0	84	89	86	FC	9B	BD	FA	D7	F1	BE	C5	79	EF	C4	ððâæâ³øç	.î±¥+y~										
0000	0150:	96	2D	D2	5C	5C	F4	4C	E8	24	83	93	CB	12	B1	18	04	û-ê~\~µLb	\$â0~..										
0000	0160:	94	BD	16	44	49	C3	54	36	76	A6	4A	D1	5D	4C	BE	E0	öç..DI T6	uâJðJL¥ó										
0000	0170:	FF	60	7D	96	D3	DD	9C	C7	9A	69	C0	60	C7	7F	EB	8F	'>ûE!Eâ	ÜiL'â0uâ										
0000	0180:	DE	F1	0E	CB	7F	C9	55	28	D7	23	7E	1F	98	10	00	4D	ì±..~ðrj<	î#~..j..M										
0000	0190:	53	8D	CF	14	50	32	6C	6E	82	C6	E1	06	2B	C6	22	B4	Sìx.P21n	éâB..+â''										
0000	01A0:	8A	23	ED	EB	F4	46	0F	15	02	EF	45	0A	77	59	A3	9B	è#ýùµF..	'E.uYú0										
0000	01B0:	21	54	1F	5B	DD	68	6D	07	F3	A3	77	AD	73	99	8E	70	?T..[!hm.	¾úw!süâp										
zalman\fw\UE400_firmware_1-37(NTFS).bin																													
0000	0000:	01	ED	10	47	A0	70	D3	BE	A4	B0	6B	DE	49	0E	09	67	.ý.GâPEV	ñk!i!..g										
0000	0010:	E1	87	DB	B4	37	87	4B	5A	4B	6D	28	F0	9E	88	21	CD	0ç~ 7çKZ	Km<->ê!=										
0000	0020:	94	2E	01	00	02	00	00	00	AA	C8	01	A7	67	D6	C1	18	ä...B...	~L..egí±.										
0000	0030:	CC	4D	92	1B	54	0C	38	8F	D7	D1	0E	18	14	5C	21	D1	ME.î.8â	îD...~!D										
0000	0040:	90	F8	0B	D7	6D	CB	4F	13	05	8A	C3	32	F7	6E	21	38	É°.îm~0.	..è 2.n!8										
0000	0050:	2A	C1	36	9E	26	1C	6B	BF	04	F2	EC	BC	7B	5F	A1	6C	*+6x&.kj	..=ýlç_í1										
0000	0060:	50	A4	5A	B1	13	1B	80	E2	4F	7E	A4	FC	F6	67	00	18	PñZ...Ç0	0~ñ³.g..										
0000	0070:	4C	63	63	D0	83	D1	E3	9A	F9	D6	16	88	36	1A	67	F1	Lccðâð0ü	"í.ê6.g±										
0000	0080:	BC	77	7F	A4	3D	75	3D	A9	B0	6F	0B	76	EA	3D	18	BA	2wðñ~u=0	0.u0=.										
0000	0090:	6B	F2	42	55	E8	C0	91	A8	6C	83	E1	7B	A3	E6	26	E0	k=BU³Læi	1âB<úµ&ó										
0000	00A0:	27	44	4B	90	2C	A3	55	32	00	39	12	0A	F5	19	DF	E0	'DKé..úU2	.9...S..ó										
0000	00B0:	8E	00	30	07	A7	AC	EC	EA	A5	E9	DA	9C	BA	02	0E	55	â..0..²¼ýü	ñú rE  ..U										
0000	00C0:	00	CC	19	19	71	31	85	41	B3	3F	92	15	9F	F2	CA	77	.J..q1âa	?æ.f=µv										
0000	00D0:	90	D0	BF	77	6F	E8	0A	85	88	14	2E	49	3E	22	F5	05	Eð~wcb.à	ê...I>"S.										
0000	00E0:	96	B0	C1	3A	93	23	4C	51	7C	7A	BB	CD	C3	19	10	7F	û~L:0#LQ	!zñ= ..â										
0000	00F0:	B2	8F	34	59	B7	0E	B4	F2	75	43	10	D5	5B	22	7D	86	4Yâ.. =	uC.²[">â										
0000	0100:	0E	93	D1	03	43	37	BB	D1	1C	C9	DF	95	EC	7C	73	37	.ðD.C7ñD	.r~ðý!s?										
0000	0110:	83	90	A9	EF	89	A1	2B	12	BB	52	38	C2	67	66	8F	DC	âé0'ëí+	ñR8T.fâ										
0000	0120:	29	3C	47	D6	9B	97	4F	F1	3A	01	87	DC	C6	50	18	95	<Gí0u0±	..ç..âP..ð										
0000	0130:	D7	0E	75	E0	17	83	32	A0	19	3D	46	5A	DC	44	88	DF	î.uó..â2â	..=FZ..Dê										
0000	0140:	E4	D0	84	89	86	FC	9B	BD	FA	D7	F1	BE	C5	79	EF	C4	ððâæâ³øç	.î±¥+y~										
0000	0150:	96	2D	D2	5C	5C	F4	4C	E8	24	83	93	CB	12	B1	18	04	û-ê~\~µLb	\$â0~..										
0000	0160:	94	BD	16	44	49	C3	54	36	76	A6	4A	D1	5D	4C	BE	E0	öç..DI T6	uâJðJL¥ó										
0000	0170:	FF	60	7D	96	D3	DD	9C	C7	9A	69	C0	60	C7	7F	EB	8F	'>ûE!Eâ	ÜiL'â0uâ										
0000	0180:	DE	F1	0E	CB	7F	C9	55	28	D7	23	7E	1F	98	10	00	4D	ì±..~ðrj<	î#~..j..M										
0000	0190:	53	8D	CF	14	50	32	6C	6E	82	C6	E1	06	2B	C6	22	B4	Sìx.P21n	éâB..+â''										
0000	01A0:	8A	23	ED	EB	F4	46	0F	15	02	EF	45	0A	77	59	A3	9B	è#ýùµF..	'E.uYú0										
0000	01B0:	21	54	1F	5B	DD	68	6D	07	F3	A3	77	AD	79	99	8E	70	?T..[!hm.	¾úw!yüâp										

```

buffalo\na_website\hd-lbu3-wr_rev120\firmware_C311.bin
0000 0000: BA C8 58 DF F7 C9 2C 65 CA CB 54 24 18 01 90 F7 ||Ug■  π.e 11πT$..E
0000 0010: 1B 3D 94 18 D8 C4 F7 BD B5 92 0A 3C 6C 78 35 E4 .°ö.î-.ç 4ñe.<1x5ö
0000 0020: 54 FD 00 00 42 00 00 00 3A EE 01 A7 67 D6 C1 18 T².~B...:°.ag1+.
0000 0030: 78 BC 93 1B E0 FD 39 8F 63 20 0F 18 A0 AD 20 D1 xJ6.ö²98 c...ë 0
0000 0040: 24 09 0A D7 6D CB 4F 13 05 8A C3 32 F7 6E 21 38 $.îmπ0..è|2 n†8
0000 0050: 2A C1 36 9E 92 ED 6A BF B0 03 ED BC 7B 5F A1 6C *+6×vJ1 2.2k_1l
0000 0060: E4 55 5B B1 A7 EA 81 E2 87 68 A4 FC 7A 63 00 18 8U1°000 çhñ°zc..
0000 0070: 84 67 63 D0 83 D1 E3 9A 0B DA 16 88 DA 18 67 F1 ägcðâðòü .r.ê r.g±
0000 0080: 88 76 7F A4 D9 77 3D A9 54 6D 0B 76 06 3F 18 BA èvüñ¹v=0 Tm.v.?.||
0000 0090: 43 F3 42 55 80 C1 91 A8 D8 72 E0 7B 17 17 27 0E C2BUÇ¹æc îröç...ó
0000 00A0: 17 48 4B 90 98 52 54 32 B4 C8 13 0A 41 E8 DE E0 .HKEÏRT2 ÷.AD10
0000 00B0: 3A F1 31 07 B9 8B EC EA F9 F6 DA 9C 0E F3 0F 55 :±1.11xgü ±r.f.%.U
0000 00C0: 3E C7 19 19 65 2B 85 41 A5 38 92 15 9F F2 CA 77 >ä...e+âA 80ñ.f.±w
0000 00D0: 58 21 BE 77 E5 ED 0A 85 88 14 2E 49 3E 22 F5 05 X†4wö9.à ê...I>†S.
0000 00E0: 96 B0 C1 3A 93 23 4C F1 7C 7A BB CD C3 19 3F 7F 01:±.ô#LQ uc.²1†'³â
0000 00F0: B2 8F 34 59 B7 0E B4 F2 75 43 10 D5 5B 22 7D 86 44Yâ.†= uC.²1†'³â
0000 0100: 0E 93 D1 03 7A 37 BB D1 1C C9 DF 95 EC 7C 73 37 .ôð.²7ñð .π.°öy1s7
0000 0110: 83 90 A9 EF 8A A1 2B 12 BB 52 38 C2 B7 B6 8E DC âé0°ëi+. πR8†ñâñ
0000 0120: 09 EC 46 D6 9B 97 4F F1 3A 01 87 DC C6 50 18 95 .gPíè0± .:ç.âP.0
0000 0130: D7 0E 75 E0 17 83 32 A0 19 3D 46 5A DC 44 88 DF î..uó.â2â .=FZ.ðê
0000 0140: E4 D0 84 89 86 FC 9B BD FA D7 F1 BE C5 79 EF C4 öðâéâ³°öç .î±4†v-
0000 0150: 96 2D D2 5C 5C F4 4C E8 24 83 93 CB 12 B1 18 04 û-ê-üπLb 5âðJ.
0000 0160: 94 BD 16 44 49 C3 54 36 76 A6 4A D1 5D 4C BE E0 öç.DI†T6 5âðJL¥0
0000 0170: FF 60 7D 96 D3 DD 9C C7 9A 69 C0 60 C7 7F EB 8F >0û:†fâ Üi¹.â0ü8
0000 0180: CE E8 2A 50 07 24 2D CF 3D C1 04 A7 C4 6E CB 5D 1p>p.$-x =±.°-nπ1
0000 0190: 31 4B A3 14 64 9B 2B B1 F9 E1 91 41 34 50 2D 60 1Kô.doç- πâñ1P-
0000 01A0: 8B FA F2 70 F4 C9 37 17 A5 D6 B2 02 DA A9 7D DB î=.pñ72. Níâñ4P-
0000 01B0: 1F 65 B0 18 D9 F8 F4 BB 87 D3 67 5D 51 AA 09 AE .e.¹°0ñj çEgJQ-..«

```

manufacture)

zalman\fw\UE400_firmware_1-37(FAT).bin																																		
0000	0000:	32	FF	1F	81	8E	F2	DE	E2	34	76	A0	2B	77	CC	03	E3	2	.	ü	ä	=	i	ö	4	v	á	+w	l	l	.	ö		
0000	0010:	92	A9	6E	62	37	E5	8E	48	FA	5D	58	97	8D	5F	05	E6	ff	@	n	b	7	ö	ä	H	0	l	x	ü	i	^	N	µ	
0000	0020:	84	2E	01	00	42	00	00	00	AA	C3	81	A7	67	D6	C1	18	ä	.	.	.	.	B	.	.	.	.	.	.	.	.	.	.	
0000	0030:	B0	4D	92	1B	28	0C	38	8F	AB	D1	0F	18	68	50	21	D1	ME	.	.	.	.	8	A	%	D	.	.	.	.	.	.	.	
0000	0040:	FC	FA	0B	D7	6D	CB	4F	13	05	8A	C3	32	F7	6E	21	38	ü	°	.	.	.	.	i	m	.	.	.	.	.	.	.	.	
0000	0050:	2A	C1	36	9E	5A	1C	6B	BF	70	F2	EC	D0	7D	5B	01	6C	*	l	6	x	Z	.	k	.	.	.	.	.	.	.	.	.	
0000	0060:	2C	04	5A	B1	6F	1B	80	E2	53	7E	A4	FC	FA	67	00	18	.	n	.	.	.	o	.	.	.	.	.	.	.	.	.	.	
0000	0070:	50	63	63	D0	83	D1	E3	9A	F5	D6	16	88	C2	19	67	F1	P	c	c	ä	ä	ö	ü	S	i	.	.	.	.	.	.	.	
0000	0080:	A8	77	7F	A4	C1	76	3D	A9	4C	6C	0B	76	1E	3E	18	BA	ä	w	ö	n	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	0090:	67	F2	42	55	FC	C0	91	A8	10	83	E1	7B	DF	E6	26	E0	g	=	B	U	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	00A0:	33	44	4B	90	50	A3	55	32	7C	39	12	0A	89	19	DF	E0	3	D	K	E	P	á	U	2	i	9	.	.	.	.	.	.	.
0000	00B0:	F2	00	30	07	CB	AC	EC	EA	B1	E9	DA	9C	C6	02	0E	55	=	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	00C0:	14	CC	19	19	6D	31	85	41	A7	3F	92	15	9F	F2	CA	77	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	00D0:	90	D0	BF	77	63	E8	0A	85	88	14	2E	49	3E	22	P5	05	E	ä	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	00E0:	96	B0	C1	3A	93	23	4C	51	7C	7A	BB	CD	C3	19	10	7F	ü	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	00F0:	B2	8F	34	59	B7	0E	B4	F2	75	43	10	D5	5B	22	7D	86	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	0100:	0E	93	D1	03	43	37	BB	D1	1C	C9	DF	95	EC	7C	73	37	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	0110:	83	90	A9	EF	89	A1	2B	12	0B	52	38	C2	0B	66	8F	DC	â	é	°	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	0120:	C5	3C	47	D6	9B	97	4F	F1	3A	01	87	DC	C6	50	18	95	†	<	G	i	ø	ù	0	±	:	.	.	.	.	.	.	.	.
0000	0130:	D7	0E	75	E0	17	83	32	A0	19	3D	46	5A	DC	44	88	DF	ï	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	0140:	E4	D0	84	89	86	FC	9B	BD	FA	D7	F1	BE	C5	79	EF	C4	ö	ä	ä	ä	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	0150:	96	2D	D2	5C	5C	F4	4C	E8	24	83	93	CB	12	B1	18	04	û	-	ê	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	0160:	94	BD	16	44	49	C3	54	36	76	A6	4A	D1	5D	4C	BE	E0	ö	ç	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	0170:	FF	60	7D	96	D3	DD	9C	C7	9A	69	C0	60	C7	7F	EB	8F	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	0180:	DE	F1	0E	CB	7F	C9	55	28	D7	23	7E	1F	98	10	00	4D	ì	±	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	0190:	53	8D	CF	14	50	32	6C	6E	82	C6	E1	06	2B	C6	22	B4	S	ì	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	01A0:	8A	23	ED	EB	F4	46	0F	15	02	EF	45	0A	77	59	A3	9B	è	#	ý	ù	.	.	.	.	.	.	.	.	.	.	.	.	.
0000	01B0:	21	54	1F	5B	DD	68	6D	07	F3	A3	77	AD	73	99	8E	70	!T	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Blocks 8, 9, 10, 11 same (Block=32 b.ts)



```

00 20 08 20 F9 46 08 00 F5 46 08 00 F5 46 08 00
F5 46 08 00 F5 46 08 00 F5 46 08 00 00 00 00 00
00 00 00 00 00 00 00 00 F5 46 08 00
F5 46 08 00 00 00 00 00 F5 46 08 00 F5 46 08 00
F5 46 08 00 F5 46 08 00 F5 46 08 00 F5 46 08 00
F5 46 08 00 F5 46 08 00 F5 46 08 00 F5 46 08 00
F5 46 08 00 F5 46 08 00 25 2C 08 00 39 2C 08 00
F5 46 08 00 61 13 08 00 81 13 08 00 A1 13 08 00
F5 46 08 00 F5 46 08 00 F5 46 08 00 F5 46 08 00
F5 46 08 00 F5 46 08 00 79 0F 08 00 F5 46 08 00
F5 46 08 00 F5 46 08 00 F5 46 08 00 F5 46 08 00
F5 46 08 00 81 36 08 00 F5 46 08 00 10 B5 05 4C
23 78 33 B9 04 4B 13 B1 04 48 AF F3 00 80 01 23
23 70 10 BD 54 0E 00 20 00 00 00 00 E8 B9 08 00
08 B5 06 4B 1B B1 06 48 06 49 AF F3 00 80 06 48
03 68 13 B1 05 4B 03 B1 98 47 08 BD 00 00 00 00
E8 B9 08 00 58 0E 00 20 E8 B9 08 00 00 00 00 00
10 B4 89 01 43 18 02 24 44 50 4F F0 FF 31 99 62
19 6A 5A 60 5D F8 04 4B 70 47 00 BF 89 01 05 23
43 50 70 47 89 01 02 23 43 50 70 47 00 EB 81 11
CA 61 70 47 00 EB 81 11 4A 62 70 47 00 EB 81 11
08 6A 70 47 70 B5 86 B0 05 46 0E 46 04 23 00 93
0C 48 0E 21 0F 22 02 AB 0B 4C A0 47 02 46 60 B9
04 2E 28 BF 04 26 4E B1 B1 00 00 23 02 AC 1C 59
EC 50 04 33 8B 42 F9 D1 00 E0 10 22 10 46 06 B0
70 BD 00 BF 00 08 0E 40 01 00 00 20 00 23 43 60
03 60 83 60 70 47 00 BF 10 B4 04 68 01 34 80 2C
28 BF 00 24 04 E0 1A B9 83 68 01 33 83 60 06 B0

```

**Figure 2.2. Vector table**

Exception number	IRQ number	Offset	Vector
16+n	n	0x0040+4n	IRQn
.	.	.	.
.	.	.	.
18	2	0x004C	IRQ2
17	1	0x0048	IRQ1
16	0	0x0044	IRQ0
15	-1	0x0040	Systick
14	-2	0x003C	PendSV
13		0x0038	Reserved
12			Reserved for Debug
11	-5		SVCall
10		0x002C	
9			Reserved
8			
7			
6	-10		Usage fault
5	-11	0x0018	Bus fault
4	-12	0x0014	Memory management fault
3	-13	0x0010	Hard fault
2	-14	0x000C	NMI
1		0x0008	Reset
		0x0004	
		0x0000	Initial SP value

On system reset, the vector table is fixed at address 0x00000000.

# Knowledge?

- Direct ARM Cortex M3 code, with stream cipher.
- Break stream cipher, all is lost.



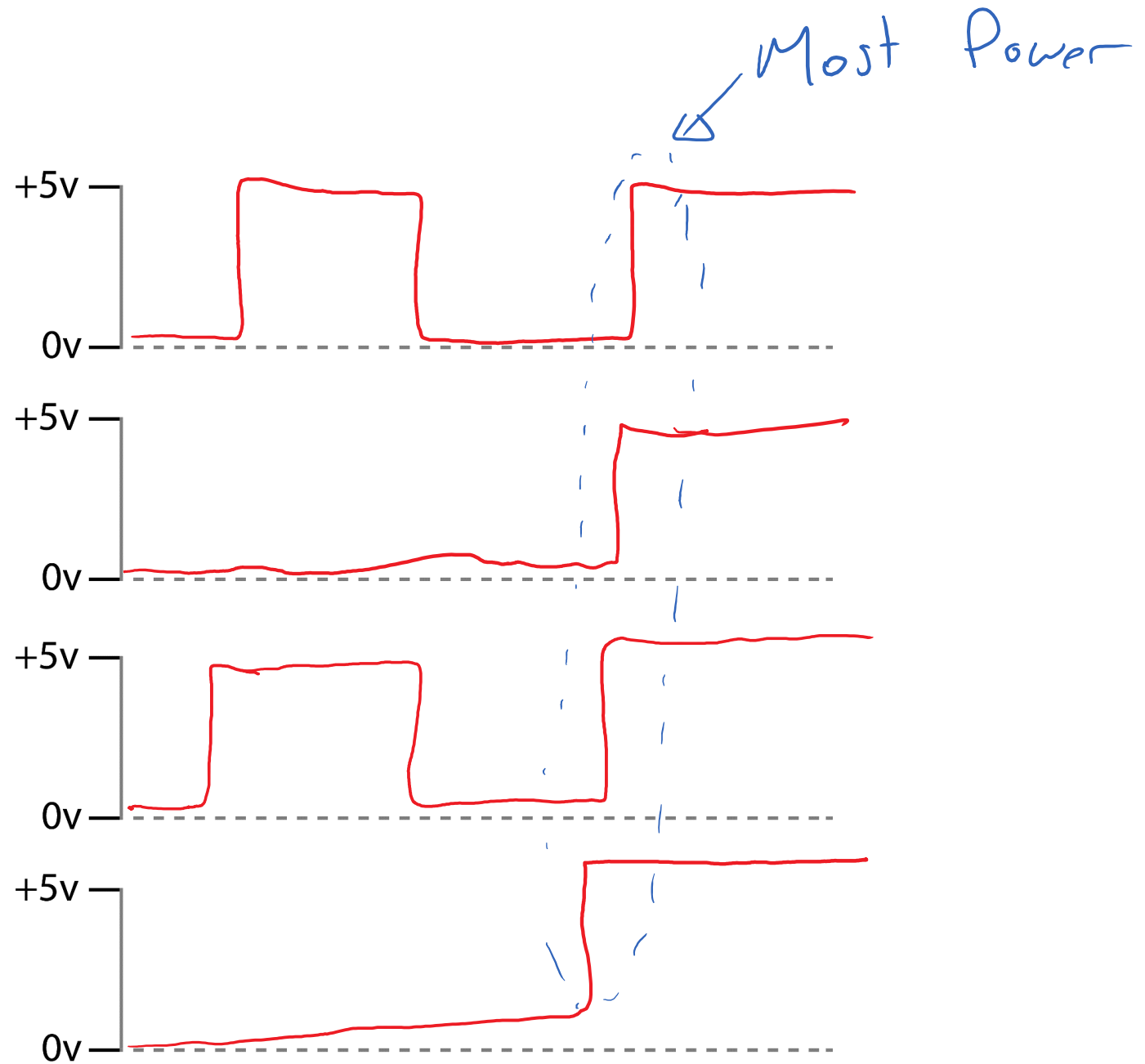


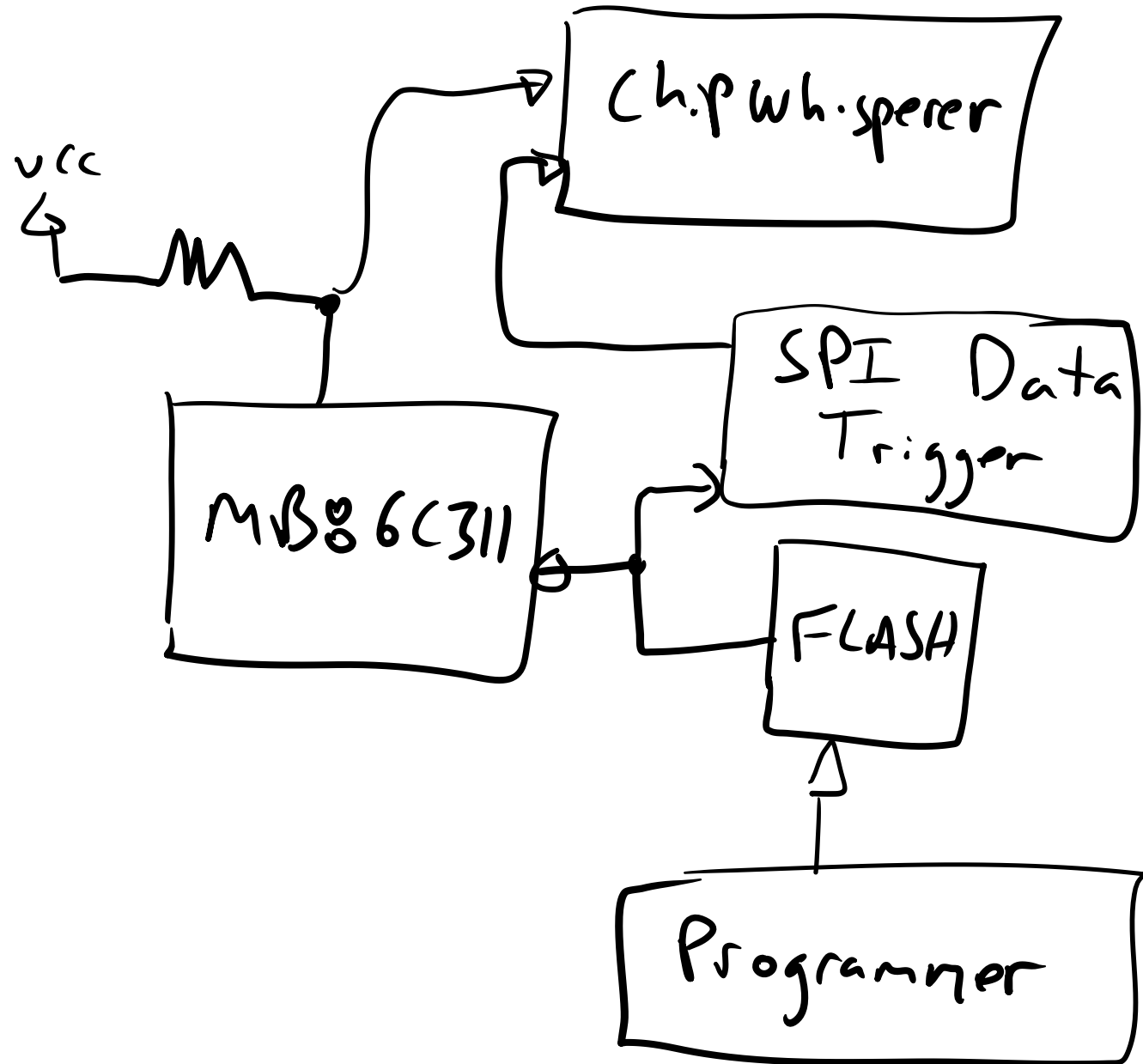
POWER

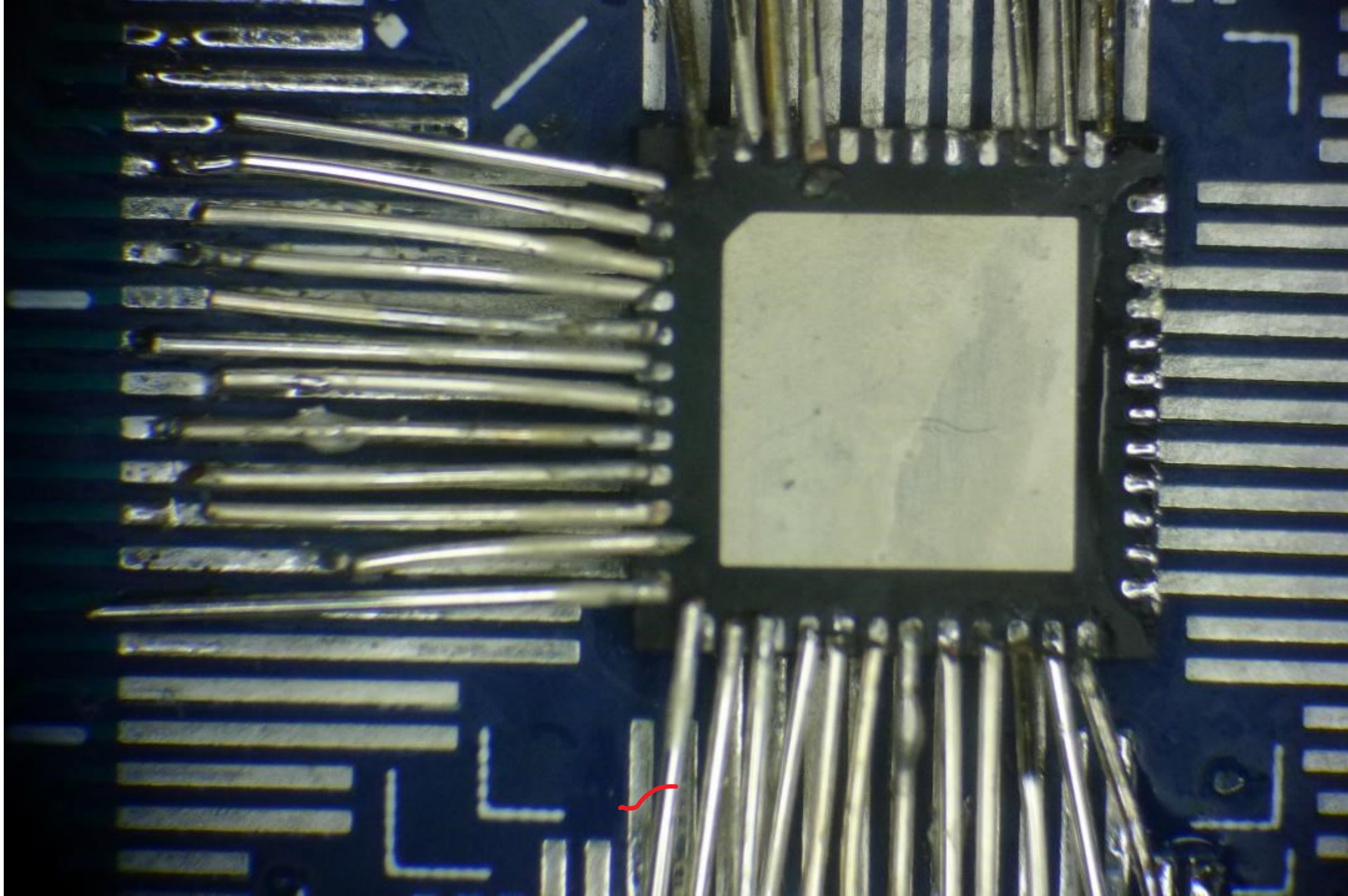
ANALYSTS?



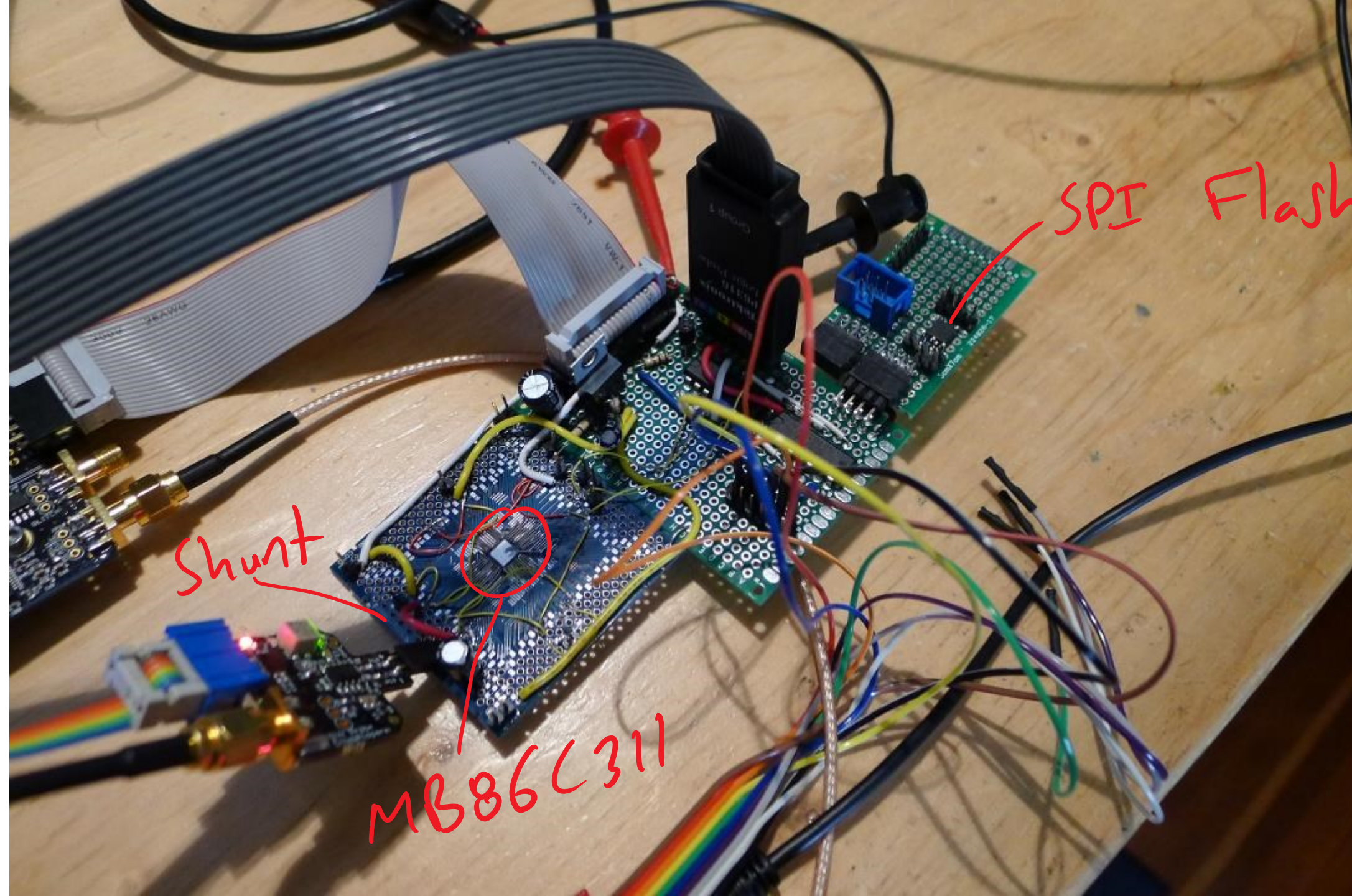
# Data Busses...









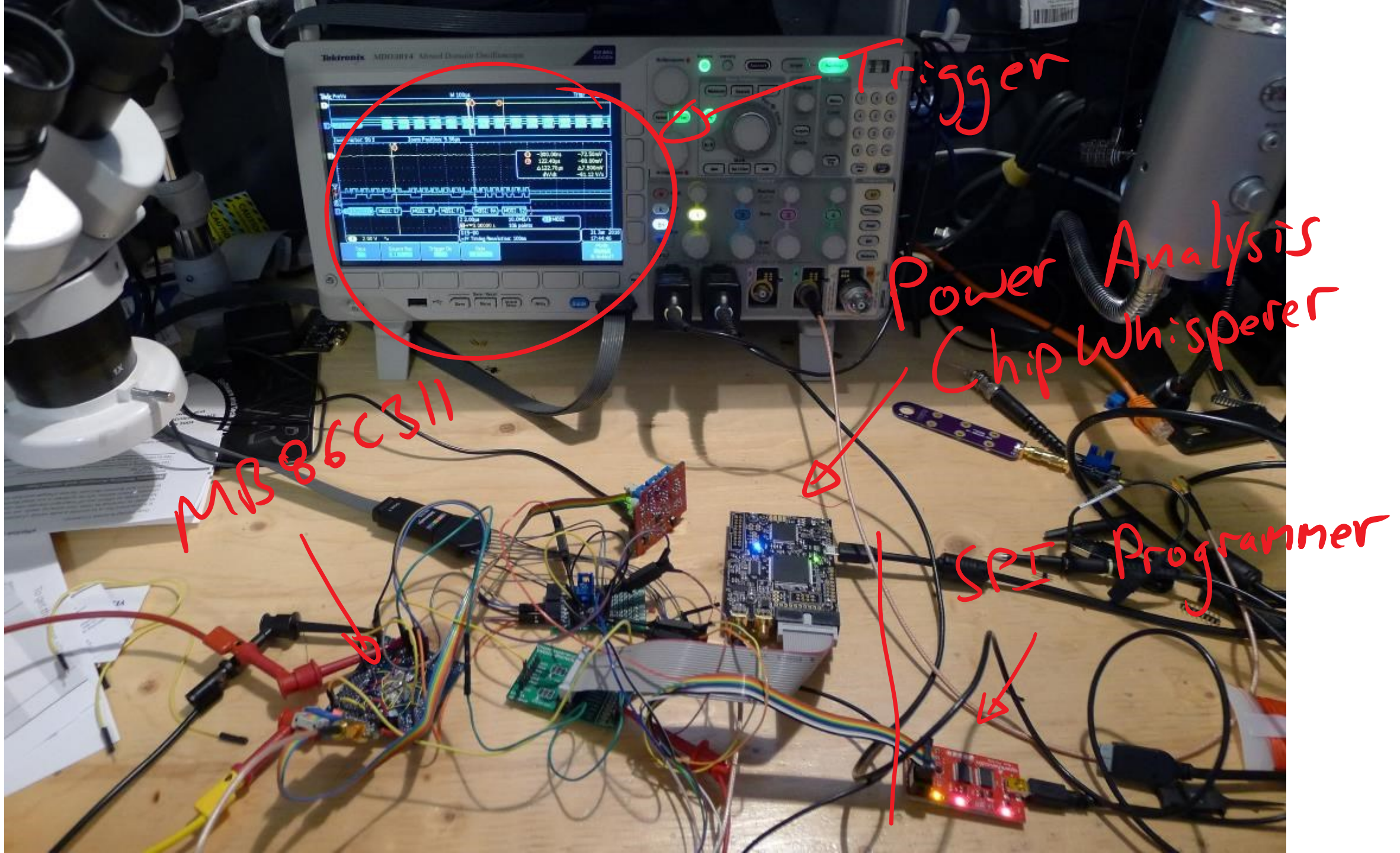


Shunt

MB86C311

SPI Flash





Trigger

Power Analysis  
Chip Whisperer

MB86C311

SPI Programmer





# POWER ANALYSIS

1. Program SPI Flash with pattern.
2. Reset MB86711, will reload FLASH.
3. Capture power at different places

## INVALID SPI DATA

Flash  
SPI loading

A

Reset released

4

200mV

~

100ms

10.0MS/s

B2 MOSI

0.000000 s

10M points

D15-D0

Timing Resolution: 100ns

21 May 2016

14:40:37

# VALID SPI DATA

Flash  
SPI loading

B

C

Reset released

4 200mV ~

100ms

10.0MS/s

B2 MOSI

0.000000 s

10M points

D15-D0

Timing Resolution: 100ns

21 May 2016  
14:44:09



# COMPARISON

Invalid = Changed a few bytes  
Valid = Original Image

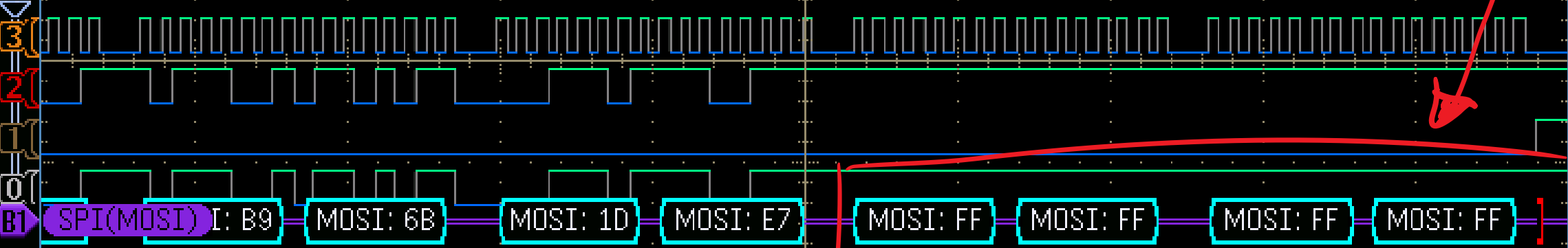
- ① Both complete operation "A"
- ② Only valid code completes "B"
- ③ Assume "C" is switching to operating code, maybe powering on SATA etc?

# LEARNING

As  $(A) \rightarrow (B)$  when code valid  
 $(A) \not\rightarrow$  when code invalid

$(A) =$  Validation (Hash?)

Experiment with "Known"  
Section where plaintext = 0's



2.00µs 2.50GS/s B1 MOSI  
0.000000 s 1M points

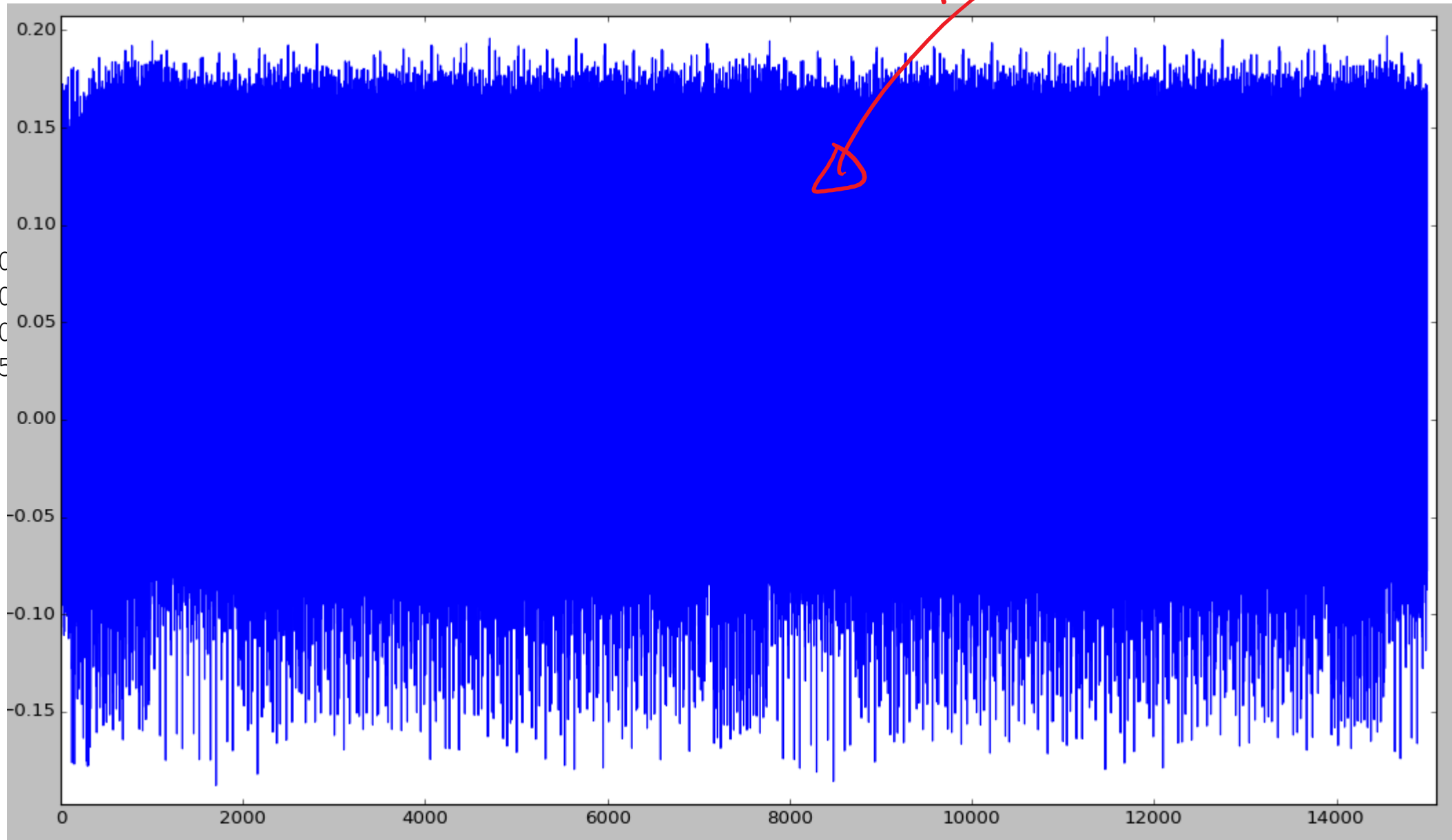
D15-D0  
Timing Resolution: 2.00ns

2 Feb 2016  
14:22:31



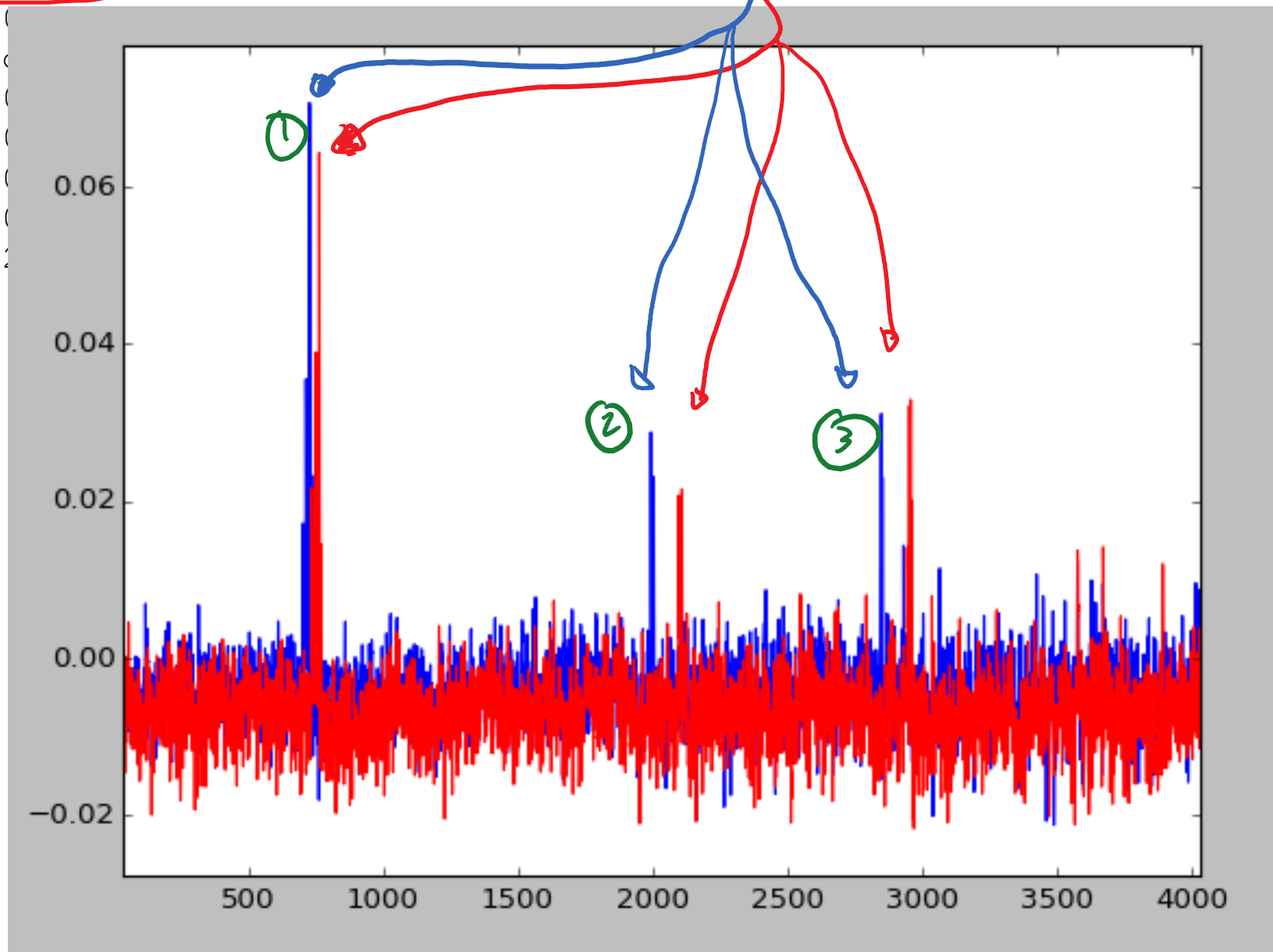
```
0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1: ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00
2: 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00
3: ff 00 00
4: 00 ff 00
5: 00 00 ff
6: 00 00 00
7: 70 0e 75
8: 8f f1 8a
9: 00 00 00
10: 00 00 00
11: 00 00 00
12: 00 00 00
13: a3 3c f5
```

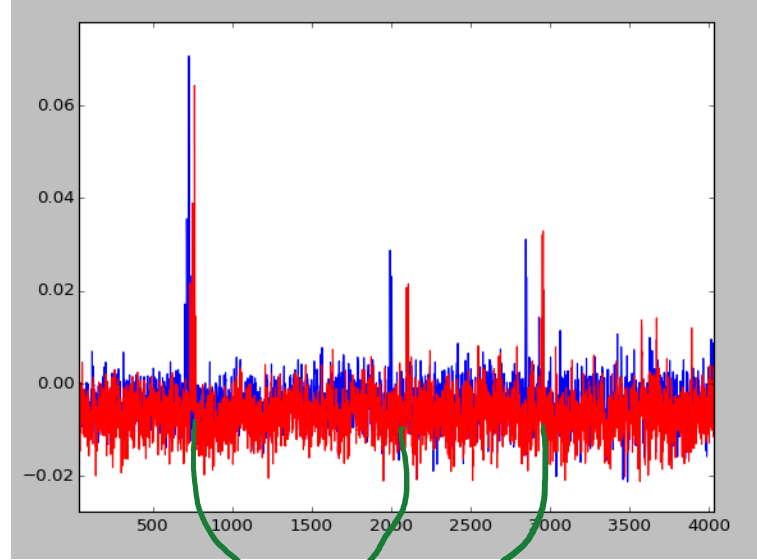
Raw power trace



0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
1: ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
2: 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00  
3: ff 00 00 00  
4: 00 ff 00 00  
5: 00 00 ff 00  
6: 00 00 00 ff  
7: 70 0e 75 ad  
8: 8f f1 8a 52  
9: 00 00 00 00  
10: 00 00 00 00  
11: 00 00 00 00  
12: 00 00 00 00  
13: a3 3c f5 54

# Difference Traces

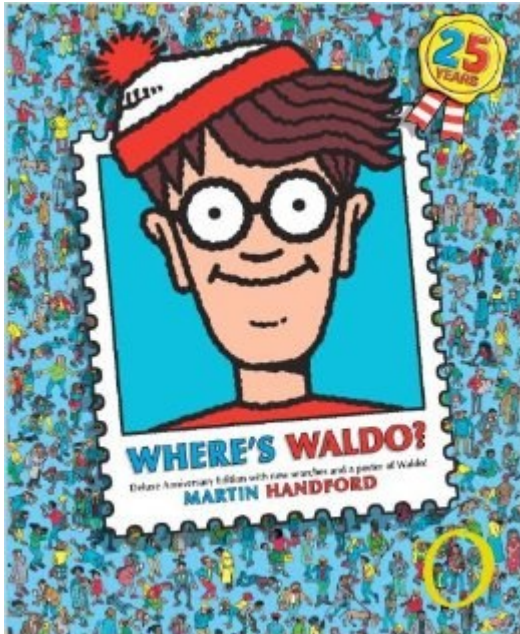




Multiple Manipulations  
↳ Some sort of feedback?



# FINDING HASH



```
#Simple python script to try a bunch of hashes
import hashlib
raw_data = open('firmware_C311.bin', 'rb').read()
known_hash = raw_data[0:32]

test_hash = hashlib.algorithms_available

for startoffset in range(0x20, 0x28, 4):
    #Trim bytes off end, seems to be some header at end?
    for endoffset in range(0, -1024, -1):
        firmware = raw_data[startoffset:endoffset]
        for t in test_hash:
            h = hashlib.new(t)
            h.update(firmware)
            dig = h.hexdigest()

            #This example uses known hash, NOT read from start of file
            #If searching in middle, do:
            #if "77badb" in dig:
            if dig.startswith("77badb"):
                print dig
                print "****HASH FOUND****"
                print "start=0x%02x, end=0x%02x, type=%s"%(startoffset, endoffset, t)
```

# BUILD SIGNATURES

```
import hashlib

fd = open('lockdown_hdd1.bin', 'rb')
orig_flash = fd.read()
fd.close()

#As an example - write 0xff's in blanks
programmed_file = [0xff]*16

newdata = orig_flash[:]
newdata = [ord(d) for d in newdata]
for i in range(0x2044, 0x2044+16):
    newdata[i] = programmed_file[i-0x2044]

#Calculate new hash
newdata_temp = ''.join([chr(j) for j in newdata])
h = hashlib.new("sha256")
h.update(newdata_temp[0x2020:0x170F8])
shash = h.hexdigest()

#Add hash to file
i=0
for t in range(0, len(shash), 2):
    newdata[0x2000+i] = int(shash[t:(t+2)], 16)
    i += 1

#Save file
newdata = ''.join([chr(j) for j in newdata])

fd = open('lockdown_temp.bin', 'wb')
fd.write(newdata)
fd.close() |
```

- 128 words per "block"
- 512 bytes

Difference  
traces

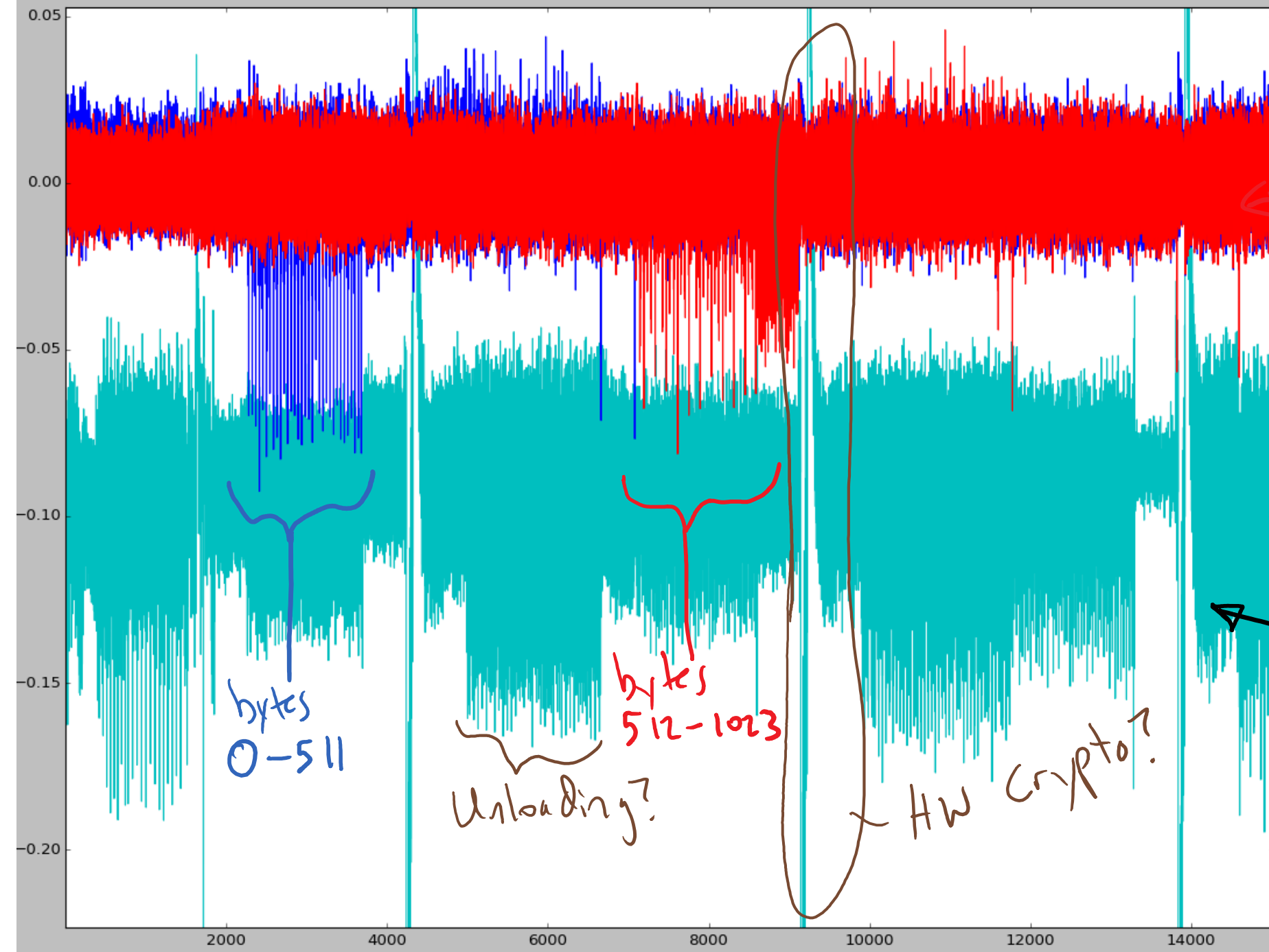
Decryption  
power  
trace

bytes  
0-511

bytes  
512-1023

Unloading?

HW crypto?





# FIRMWARE ATTACKS

- 1) Can cause arbitrary code to be decrypted.
- 2) Can move interrupt/reset vectors quazi-blindly.
- 3) If could determine either (a) part of stream cipher or (b) part of code (init routines?) may be able to build short "dumper".

# HARD DRIVE SUMMARY

1. No secrets inside silicon
  2. Secure and normal variants of.  
MB86C311 use same FW protection.
- ∴ Any company using these devices  
could decrypt this FW.

# HARD DRIVE SUMMARY

3. Once F.W. is known,  
all is lost. Possible to  
Brute-force password in  $< 1s$ .
4. Various attack vectors to FW  
itself due to flaws.



# QUESTIONS?

**Colin O'Flynn**

@colinoflynn

oflynn.com


newae.com

coflynn@newae.com

Twitter



Website / Blog



Company

