Key-Logger, Video, Mouse

How to turn your KVM into a raging key-logging monster

Check Point
SOFTWARE TECHNOLOGIES LTD.

MEETTHETEAM

Yaniv Balmas

“This should theoretically work”

Security Researcher

Check Point Software Technologies

@ynvb

Lior Oppenheim

“The mad scientist”

Security Researcher

Check Point Software Technologies

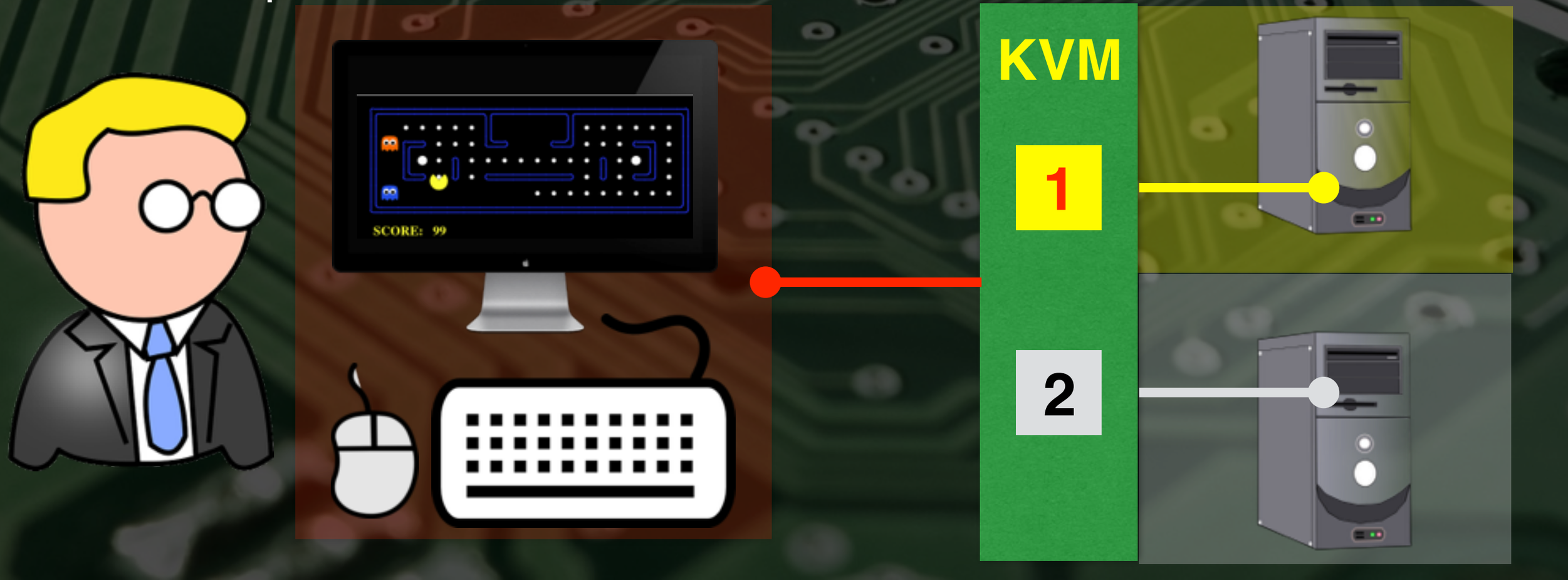
@oppenheim1

TOOMANYCOMPUTERS

- Computers
- Many computers
- **A LOT OF COMPUTERS**

WHATISKVM?

- **K**eyboard, **V**ideo, **M**ouse
- KVM connects the same Keyboard, Video and Mouse to one or more computers.



WHEREARETHEY?

- On your desktops.
- In your server racks.
- In *very* secure environments.

KVMS ARE EVERYWHERE!!

KVMEVOLUTION

`A-B Switch` Modern KVM Matrix KVM

1990

4 Ports

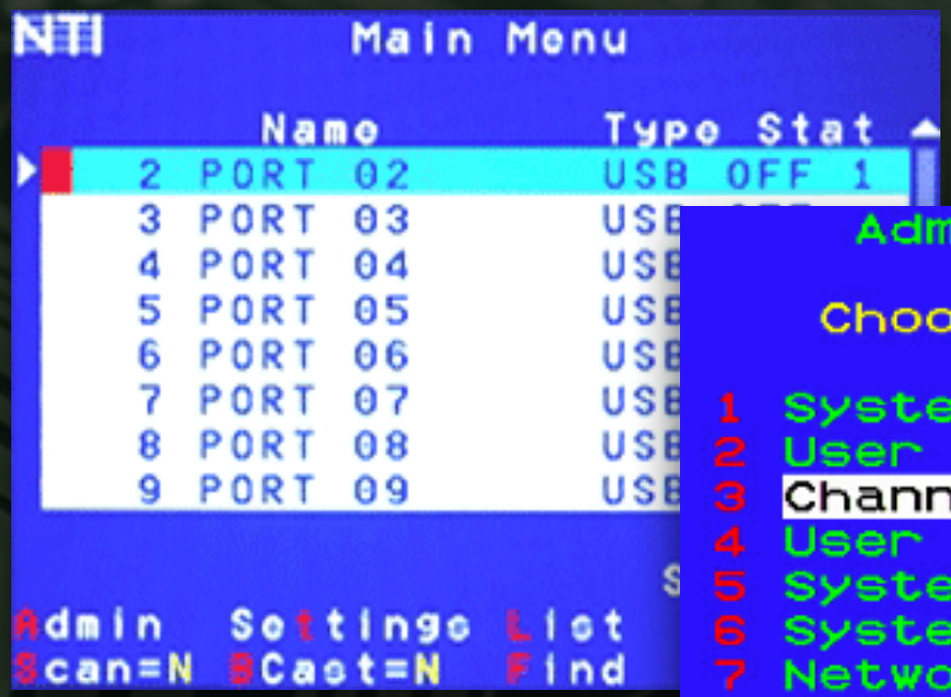
2000

16 Ports

2010

1024+ Ports

STUPIDBOXES?



IT RUNS CODE!!

WHATCANWEDO?

- What's the one common thing here?
- All features require the KVM to process key-strokes!
- If we could "theoretically" control the key processing routine…

KEY-LOGGER

SOFTWARE

- Manuals, Cables, Warranty and a CD…
- CD contains some interesting files:
  - A Firmware Upgrade Utility.
  - firmware.bin
- Since x86 is no new territory, we can reverse engineer this!

MEETTHEBLOB

FAIL!

SERIALSNIFF

- Firmware upgrade process is done via a custom serial protocol.
- It is possible to extract the (possibly) encoded firmware binary from the serial protocol.
- It’s just a matter of analyzing the serial protocol.

PROTOCOLANALYSIS

Handshake

```
46 55 90 00 44 49 b8                                    FUê.DI╖
46 55 10 00 43 ** 2d 31 ** ** 34 41 2f 31 ** **         FU..C*-1**4A/1**
32 41 00 00 4d 41 49 4e 00 00 00 56 34 32 52 34         2A..MAIN...V42R4
31 37 56 31 30 52 30 38 31 57 37 38 45 36 35 00         17V10R081W78E65.
00 a2                                                   .¢
46 55 a0 00 43 54 d2                                    FU†.CT“
46 55 20 00 00 bb                                       FU .. ª
46 55 a2 00 ** ** ** ** ** ** 2d 31 37 33 ** 41         FU¢.******-173*A
2f 31 ** ** ** 41 00 00 4d 41 49 4e 00 00 00 56         /1***A..MAIN…V
34 32 56 31 30 04 ce 19 a7 75 50 35 ca aa 6a 0a         42V10.Œ.ßuP5 ™j.
ca 8a 0a aa 01 09 8c 69 73 49 1c c0 6a c7 01 ac          ä.™..åisI.¿j«.¨
7f 25 25 49 10                                          %%I.
46 55 22 00 00 bd                                       FU".. Ω
46 55 a3 00 00 00 05 68 70 7d 5b af 65 05 4d ea         FU£....hp}[Øe.MÍ
2d a1 4f 55 85 05 d1 04 04 b7 d8 76 05 05 7a 04         -°OUÖ.—..∑ÿv..z.
04 84 e3 17 04 05 04 04 04 ba 15 ed 32 05 ec 68         .Ñ„.......∫.Ì2.Ïh
03 0f 8b 0f be 85 16 37 be 12 85 07 13 c5 b7 96         ..ã.æÖ.7æ.Ö..≈∑ñ
92 03 94 7f 05 3d 2a                                    í.î.=*
```

Data Transfer

```
46 55 a3 00 03 63 40 d7 85 85 32 ea e2 01 6b 85         FU£..c@◊ÖÖ2Í,.kÖ
32 a6 d9 d6 e5 df 55 a6 d5 22 04 d6 cd 05 d5 96         2¶Ÿ÷ÂflU¶’".÷Õ.’ñ
27 85 85 d7 40 a5 d7 32 01 32 e2 85 6b ea 85 d9         'ÖÖ◊@•◊2.2,ÖkÍÖŸ
df d5 e5 a6 55 d6 a6 04 2d 27 cd 22 d5 d6 96 85         fl’Â¶U÷¶.-'Õ"’÷ñÖ
a5 01 40 85 d7 d7 81                                    •.@Ö◊◊Å
46 55 23 00 03 63 00 24                                 FU#..c.$
```

- From KVM
- To KVM
- Fixed Header
- OpCode
- Seq. Number
- CheckSum

GUESSWHO?

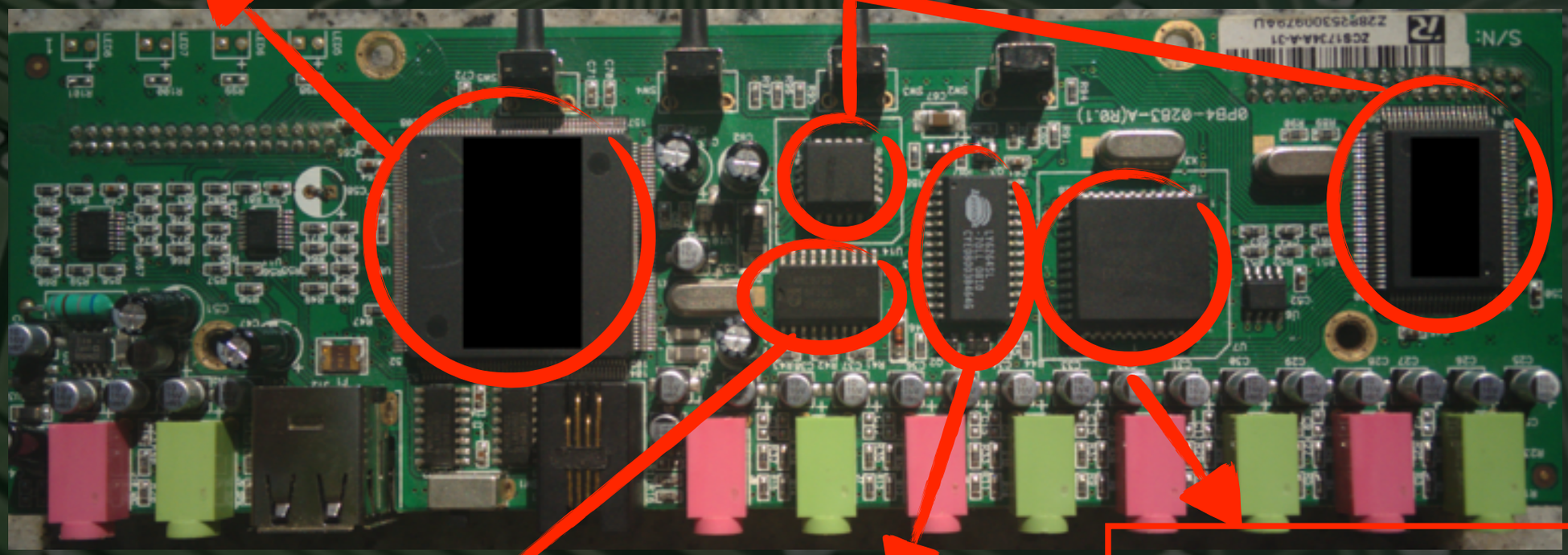
0000h:	CD	23	32	43	65	43	06	3B	33	C3	AC	43	19	0B	6B	F7	Í#2CeC.;3Ã¬C..k÷
0010h:	14	43	42	43	E6	E3	42	C1	B6	42	42	43	8D	DC	42	C2	.CBCæãBÁ¶BBC.ÜBÂ
0020h:	AB	74	42	43	53	42	42	FC	AE	F8	2E	C3	D5	AA	45	49	«tBCSBBü®ø.ÃÕªEI
0030h:	51	75	71	83	C3	50	F8	54	31	43	D0	7B	D2	F1	D4	45	QuqƒÃPøT1CÐ{ÒñÔE
0040h:	53	BC	11	4B	43	31	D2	D7	4E	54	54	D0	43	E3	D4	D0	S¼.KC1Ò×NTTÐCãÔÐ
0050h:	D0	43	E3	C4	54	EB	D7	4E	C4	C3	3B	D7	E3	54	D0	41	ÐCãÄTë×NÄÃ;×ãTÐA
0060h:	71	5B	51	75	54	4A	C3	D4	43	4E	81	54	D0	D7	EB	54	q[QuTJÃÔCN.TÐ×ëT
0070h:	54	D0	D7	EB	B1	D0	EB	43	EB	B1	D0	3B	D7	4E	54	C3	TÐ×ë±ÐëCë±Ð;×NTÃ
0080h:	54	71	C3	51	75	41	4A	43	D0	43	EB	75	54	D4	D7	4E	TqÃQuAJCÐCëuTÔ×N
0090h:	65	54	EB	D7	EB	54	D0	D0	D7	EB	54	D0	3B	43	4E	65	eTë×ëTÐÐ×ëTÐ;CNe
00A0h:	75	54	4A	C3	51	C3	41	71	54	D0	D7	93	22	73	D4	43	uTJÃQÃAqTÐ×"sÔC
00B0h:	93	D2	D0	EB	D7	4E	54	54	3B	D7	4E	54	D0	D0	43	93	"ÒÐë×NTT;×NTÐÐC"
00C0h:	51	75	41	4A	C3	D2	C3	54	C4	54	D4	D7	E3	71	13	D0	QuAJÃÒÃTÄTÔ×ãq.Ð
00D0h:	D0	62	54	70	5B	73	4E	D7	4E	54	54	D0	73	EB	B1	70	ÐbTp[sN×NTTÐsë±p
00E0h:	65	54	83	D7	EB	5B	D0	D0	D0	23	54	70	5B	73	4E	D7	eTƒ×ë[ÐÐÐ#Tp[sN×
00F0h:	4E	54	54	D0	73	93	D2	70	74	FC	43	C5	11	5B	D0	AA	NTTÐs"ÒptüCÅ.[Ðª
0100h:	51	4B	4D	FF	93	7C	AA	43	93	A1	45	2E	D7	23	4E	7C	QKMÿ"|ªC"¡E.×#N|
0110h:	F8	49	C3	41	A5	AA	D4	50	75	54	83	C3	51	F8	71	AC	øIÃA¥ªÔPuTƒÃQøq¬
0120h:	57	43	16	63	13	26	AA	4D	4B	43	B4	52	74	CB	95	23	WC.c.&ªMKC´RtË•#
0130h:	AA	76	D4	00	7C	10	F8	72	F2	E3	47	7C	D4	D4	FC	FC	ªvÔ.|.øròãG|ÔÔüü
0140h:	21	50	A4	4E	54	4F	54	4B	50	F8	10	F8	49	43	23	71	!P¤NTOTKPø.øIC#q
0150h:	AA	D4	51	75	7C	D3	C3	AC	16	6B	81	54	A4	D7	93	13	ªÔQu|ÓÃ¬.k.T¤×".
0160h:	B4	D2	4D	CB	95	57	43	54	FC	47	E1	7A	AA	7A	F0	74	´ÒMË•WCTüGázªzðt
0170h:	FC	51	FC	4F	54	F2	93	74	16	6B	2E	AA	73	FC	59	13	üQüOTò"t.k.ªsüY.
0180h:	B4	F4	4D	CA	95	57	43	A1	C3	F8	81	D4	57	D7	93	49	´ôMÊ•WC¡Ãø.ÔW×"I
0190h:	51	75	71	F4	C3	50	F8	C3	54	FC	C3	51	75	71	E5	59	QuqôÃPøÃTüÃQuqåY
FF00h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FF10h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FF20h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FF30h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FF40h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FF50h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FF60h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FF70h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FF80h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FF90h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FFA0h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FFB0h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FFC0h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FFD0h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FFE0h:	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	53	SSSSSSSSSSSSSSSS
FFF0h:	53	53	53	53	53	53	53	53	E1	F2	F2	DA	FA	53	C1	C2	SSSSSSSáòòÚúSÁÂ
0000h:																	

FAIL!

PCBLAYOUT

Unknown

PLD



D-Latch

2K
External
RAM

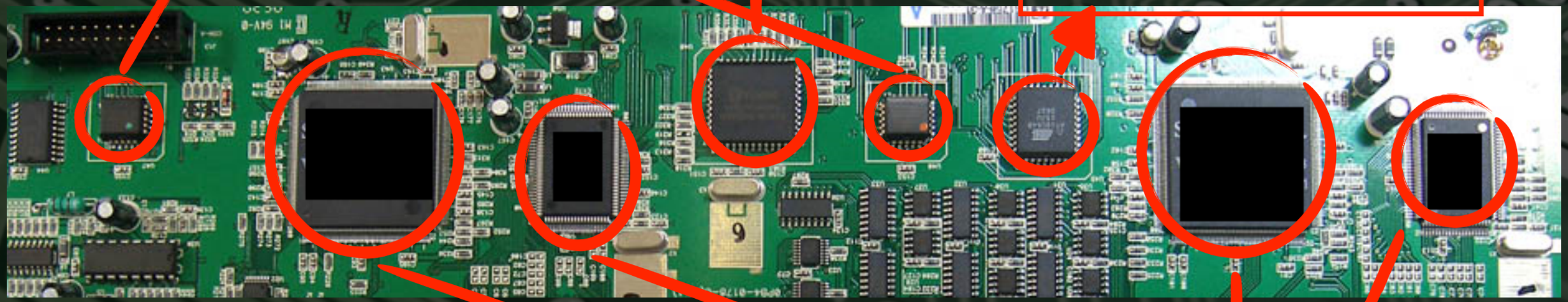
8052
Processor

PCBLAYOUT

PLD X2

8052 X1

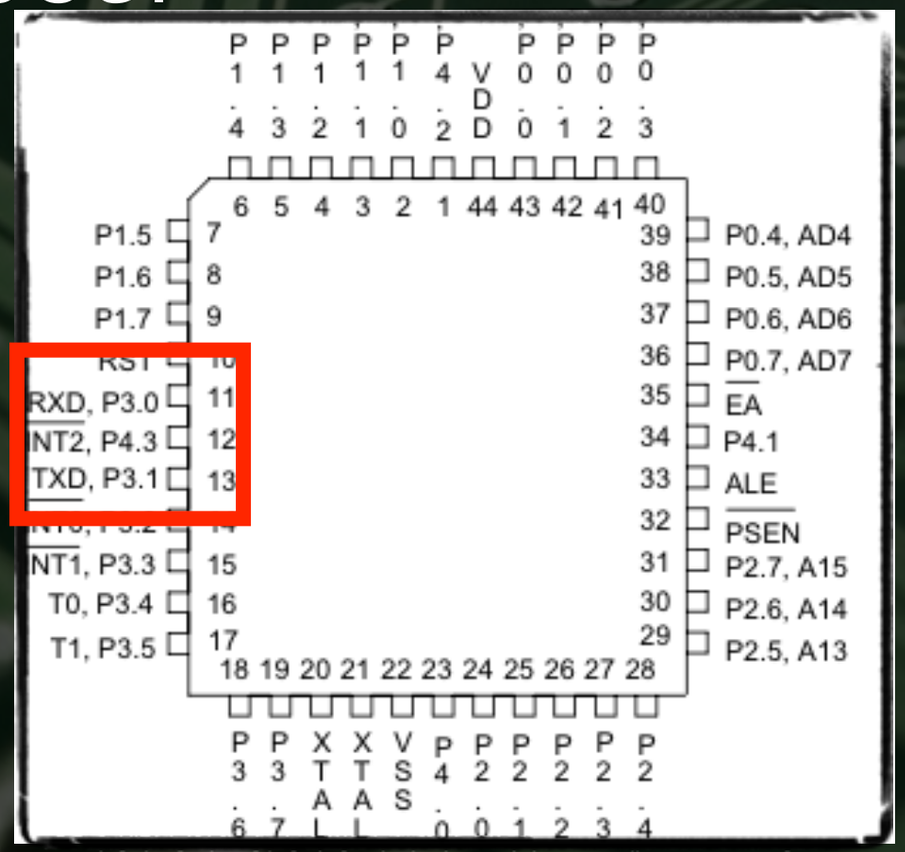
External
RAM X1

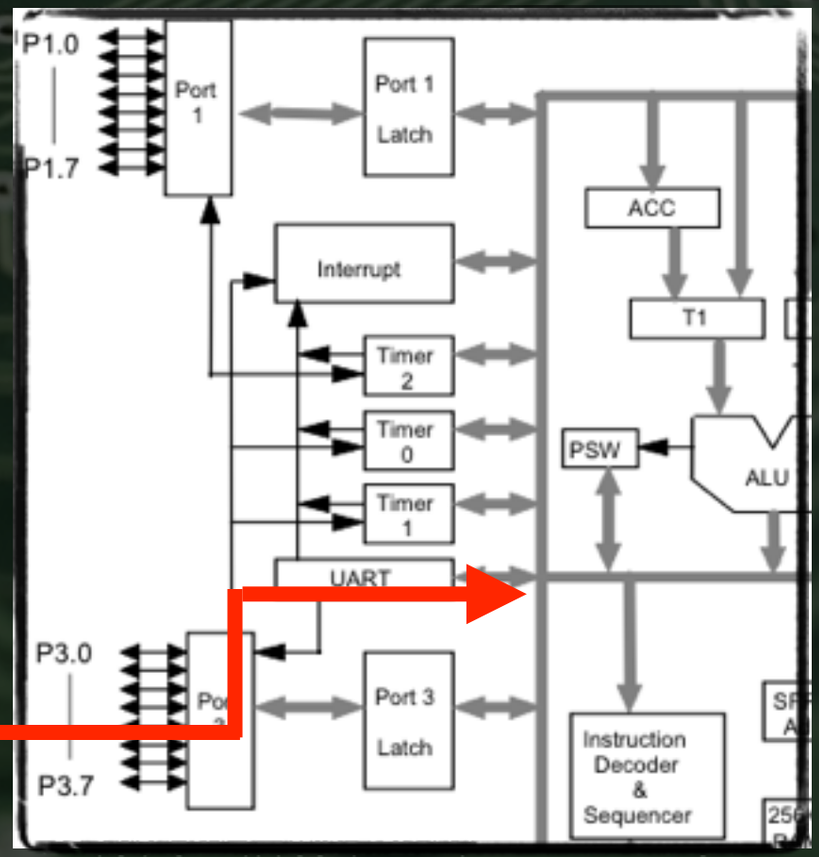


Unknown
X2

UARTMAGIC

- 8051\2 Chips have an integrated UART port.
- Which IC pins should be tapped?
- In order to find out, let's take a look at the specs.



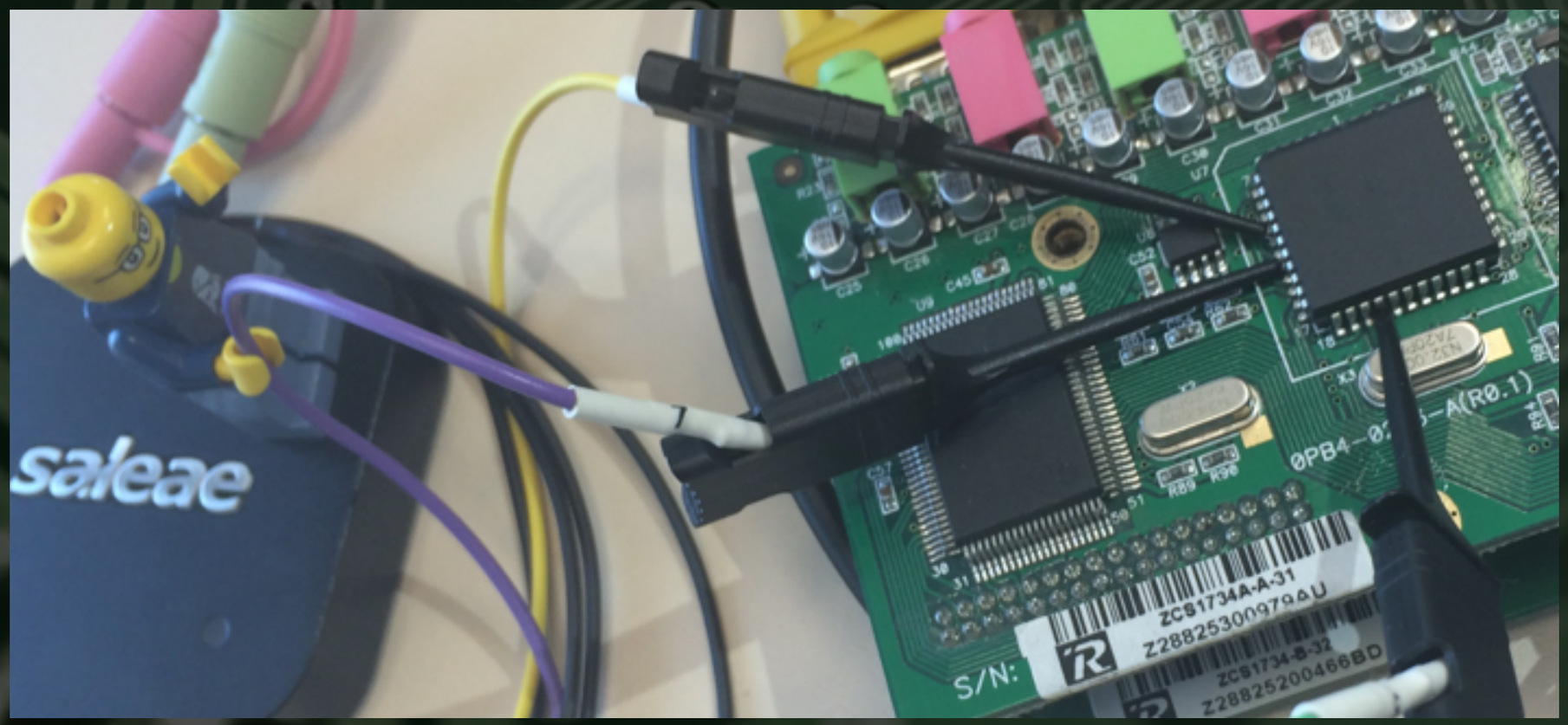


NOTHINGBUTLOGIC

- 30-45 China mail shipping days later.
- We can finally use LOGIC.

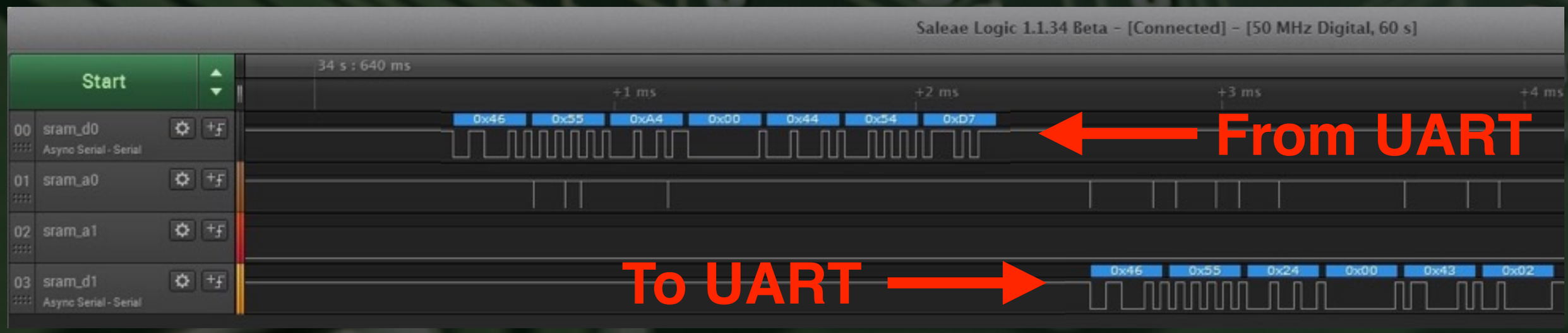
TAPICPINS

- Tapping the 8052 IC UART pins using Logic Analyzer.
- Reveals the the UART port’s signals.



SIGNALANALYSIS

- Reviewing the signals in the UI.
- An obvious pattern emerges.



GREATFAIL!

```
46 55 90 00 44 49 b8                                    FUê.DI¶
46 55 10 00 43 ** 2d 31 ** ** 34 41 2f 31 ** **        FU..C*-1**4A/1**
32 41 00 00 4d 41 49 4e 00 00 00 56 34 32 52 34        2A..MAIN...V42R4
31 37 56 31 30 52 30 38 31 57 37 38 45 36 35 00        17V10R081W78E65.
00 a2                                                   .¢
46 55 a0 00 43 54 d2                                    FU†.CT“
46 55 20 00 00 bb                                       FU ..ª
46 55 a2 00 ** ** ** ** ** ** 2d 31 37 33 ** 41        FU¢.******-173*A
2f 31 ** ** ** 41 00 00 4d 41 49 4e 00 00 00 56        /1***A..MAIN…V
34 32 56 31 30 04 ce 19 a7 75 50 35 ca aa 6a 0a        42V10.Œ.ßuP5 ™j.
ca 8a 0a aa 01 09 8c 69 73 49 1c c0 6a c7 01 ac        Ê.™..åisI.¿j«.¨
7f 25 25 49 10                                          .%%I.
46 55 22 00 00                                          FU"..Ω
46 55 a3 00 00 00 03 68 70 7d 5b d8 65 05 4d ea        FU£....hp}[Øe.MÍ
2d a1 4f 55 85 05 d1 04 04 b7 d8 76 05 05 7a 04        -°OUÖ.—..∑ÿv..z.
04 84 e3 17 04 05 04 04 04 ba 15 ed 32 05 ec 68        .Ñ„.....∫.Ì2.Ïh
03 0f 8b 0f be 85 16 37 be 12 85 07 13 c5 b7 96        ..ã.œÖ.7œ.Ö..≈∑ñ
92 03 94 7f 05 3d 2a                                    í.î.=*
```

Or is it?

• • •

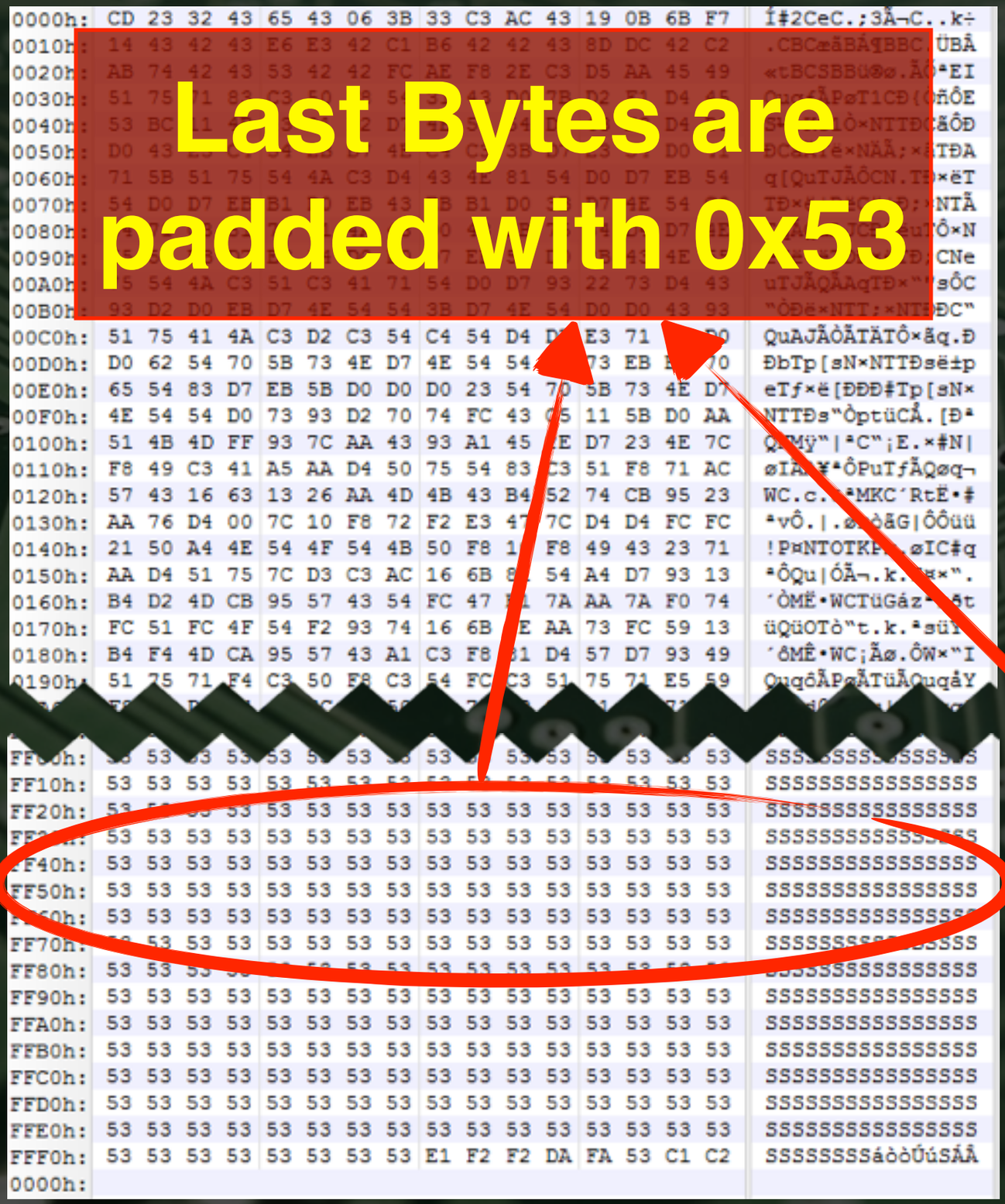
```
46 55 a3 00 03 63 40 d7 85 85 32 ea e2 01 6b 85        FU£..c@◊ÖÖ2Í,.kÖ
32 a6 d9 d6 e5 df 55 a6 d5 22 04 d6 cd 05 d5 96        2¶Ÿ÷ÂflU¶'".÷Õ.'ñ
27 85 85 d7 40 a5 d7 32 01 32 e2 85 6b ea 85 d9        'ÖÖ◊@•◊2.2,ÖkÍÖŸ
df d5 e5 a6 55 d6 a6 04 2d 27 cd 22 d5 d6 96 85        fl'Â¶U÷¶.-'Õ"'÷ñÖ
a5 01 40 85 d7 d7 81                                    •.@Ö◊◊Å
46 55 23 00 03 63 00 24                                 FU#..c.$
```

BREAKINGCODE

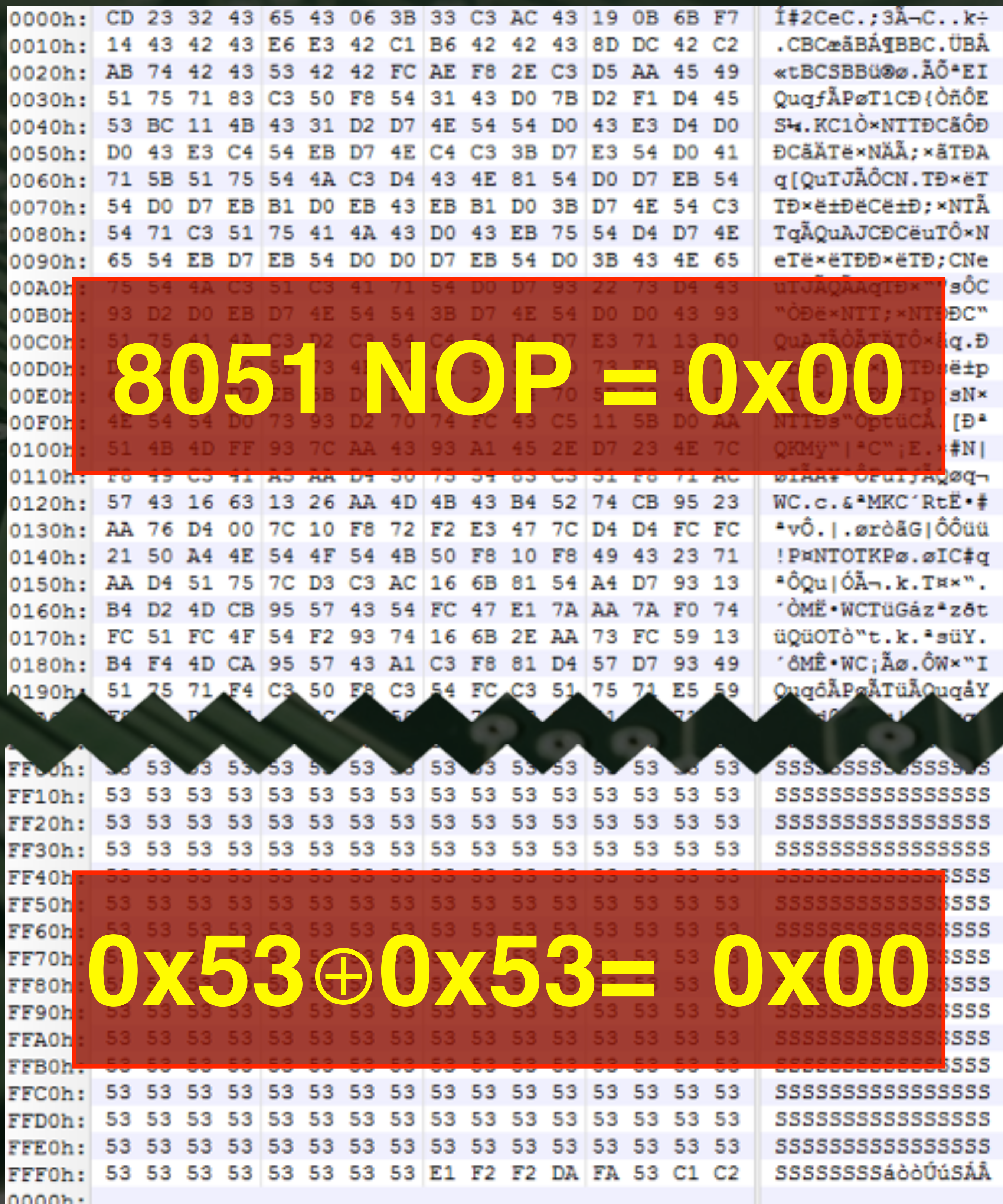
- The BLOB is probably translated into 8051 Assembly.
- The translation is done somewhere within the 8052 chip.
- It might be possible to break the obfuscation!

REMEETTHEBLOB

Last Bytes are padded with 0x53



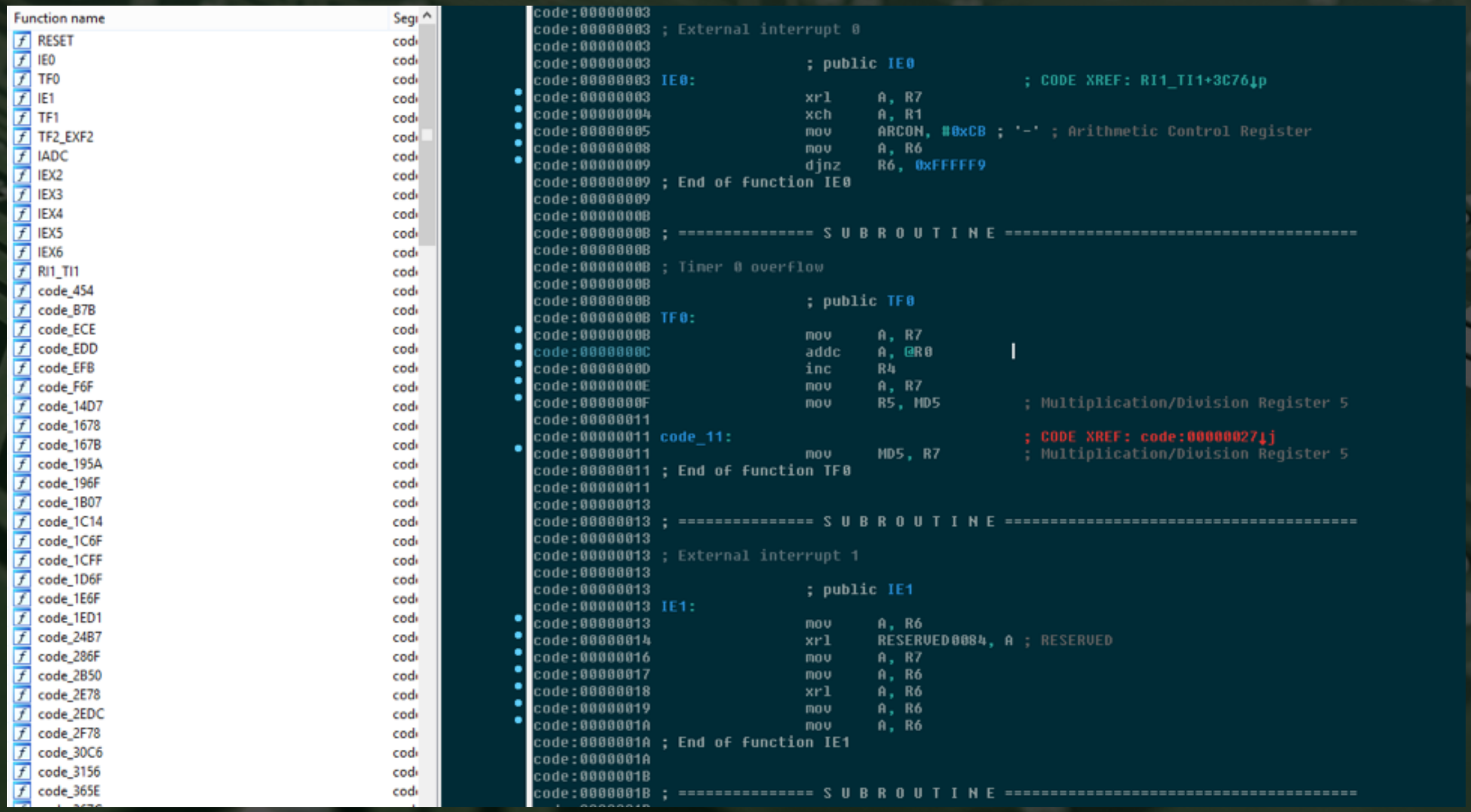
BREAKING CODE



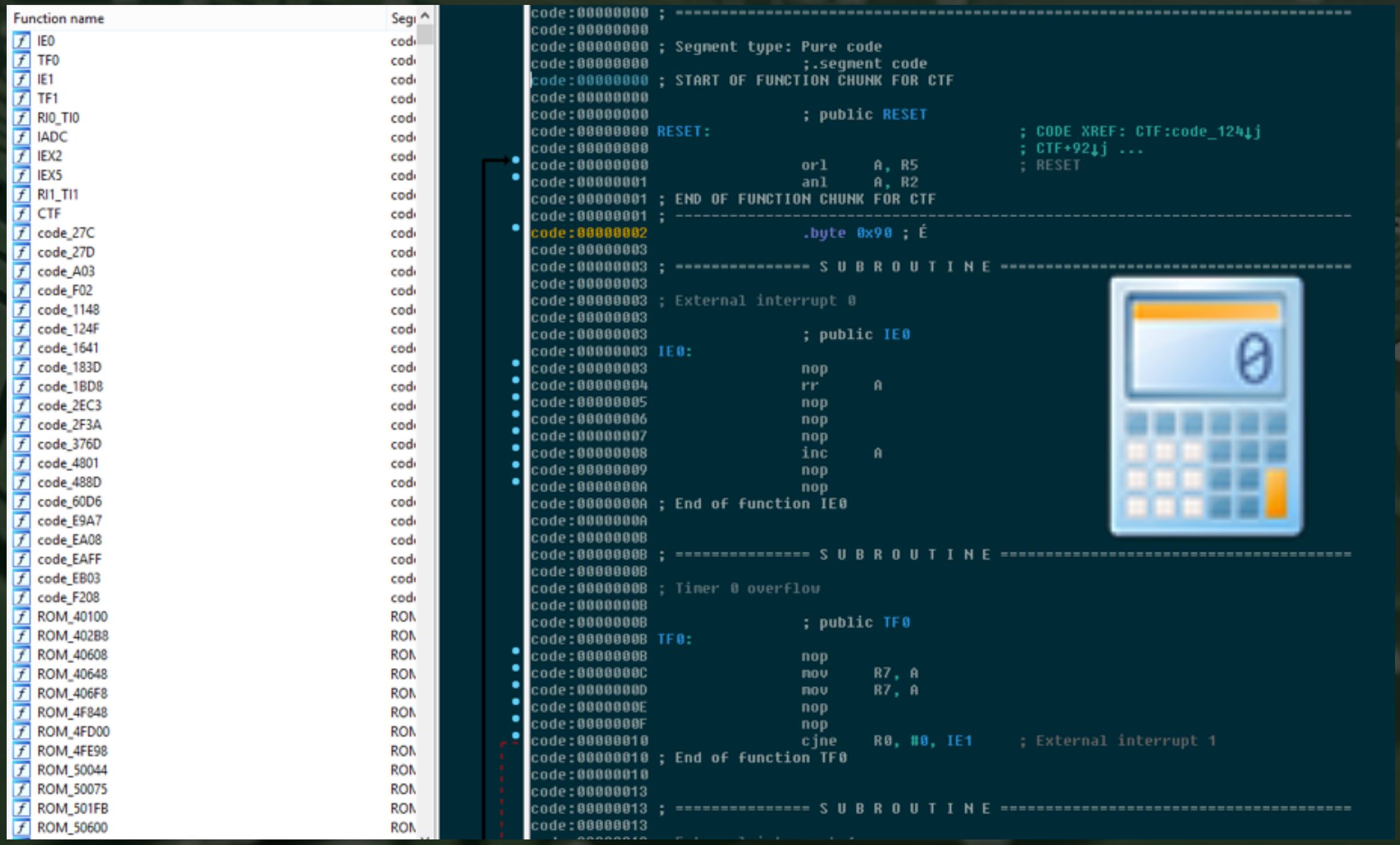
ALLDONE!

0000h:	9E	70	61	10	36	10	55	68	60	90	FF	10	4A	58	38	A4
0010h:	47	10	11	10	B5	B0	11	92	E5	11	11	10	DE	8F	11	91
0020h:	F8	27	11	10	00	11	11	AF	FD	AB	7D	90	86	F9	16	1A
0030h:	02	26	22	D0	90	03	AB	07	62	10	83	28	81	A2	87	16
0040h:	00	EF	42	18	10	62	81	84	1D	07	07	83	10	B0	87	83
0050h:	83	10	B0	97	07	B8	84	1D	97	90	68	84	B0	07	83	12
0060h:	22	08	02	26	07	19	90	87	10	1D	D2	07	83	84	B8	07
0070h:	07	83	84	B8	E2	83	B8	10	B8	E2	83	68	84	1D	07	90
0080h:	07	22	90	02	26	12	19	10	83	10	B8	26	07	87	84	1D
0090h:	36	07	B8	84	B8	07	83	83	84	B8	07	83	68	10	1D	36
00A0h:	26	07	19	90	02	90	12	22	07	83	84	C0	71	20	87	10
00B0h:	C0	81	83	B8	84	1D	07	07	68	84	1D	07	83	83	10	C0
00C0h:	02	26	12	19	90	81	90	07	97	07	87	84	B0	22	40	83
00D0h:	83	31	07	23	08	20	1D	84	1D	07	07	83	20	B8	E2	23
00E0h:	36	07	D0	84	B8	08	83	83	83	70	07	23	08	20	1D	84
00F0h:	1D	07	07	83	20	C0	81	23	27	AF	10	96	42	08	83	F9
0100h:	02	18	1E	AC	C0	2F	F9	10	C0	F2	16	7D	84	70	1D	2F
0110h:	AB	1A	90	12	F6	F9	87	03	26	07	D0	90	02	AB	22	FF
0120h:	04	10	45	30	40	75	F9	1E	18	10	E7	01	27	98	C6	70
0130h:	F9	25	87	53	2F	43	AB	21	A1	B0	14	2F	87	87	AF	AF
0140h:	72	03	F7	1D	07	1C	07	18	03	AB	43	AB	1A	10	70	22
0150h:	F9	87	02	26	2F	80	90	FF	45	38	D2	07	F7	84	C0	40
0160h:	E7	81	1E	98	C6	04	10	07	AF	14	B2	29	F9	29	A3	27
0170h:	AF	02	AF	1C	07	A1	C0	27	45	38	7D	F9	20	AF	0A	40
0180h:	E7	A7	1E	99	C6	04	10	F2	90	AB	D2	87	04	84	C0	1A
0190h:	02	26	22	A7	90	03	AB	90	07	AF	90	02	26	22	B6	0A
FF00h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FF10h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FF20h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FF30h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FF40h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FF50h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FF60h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FF70h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FF80h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FF90h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FFA0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FFB0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FFC0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FFD0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FFE0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
FFF0h:	00	00	00	00	00	00	00	00	B2	A1	A1	89	A9	00	92	91
0000h:																

8051 ASSEMBLY?

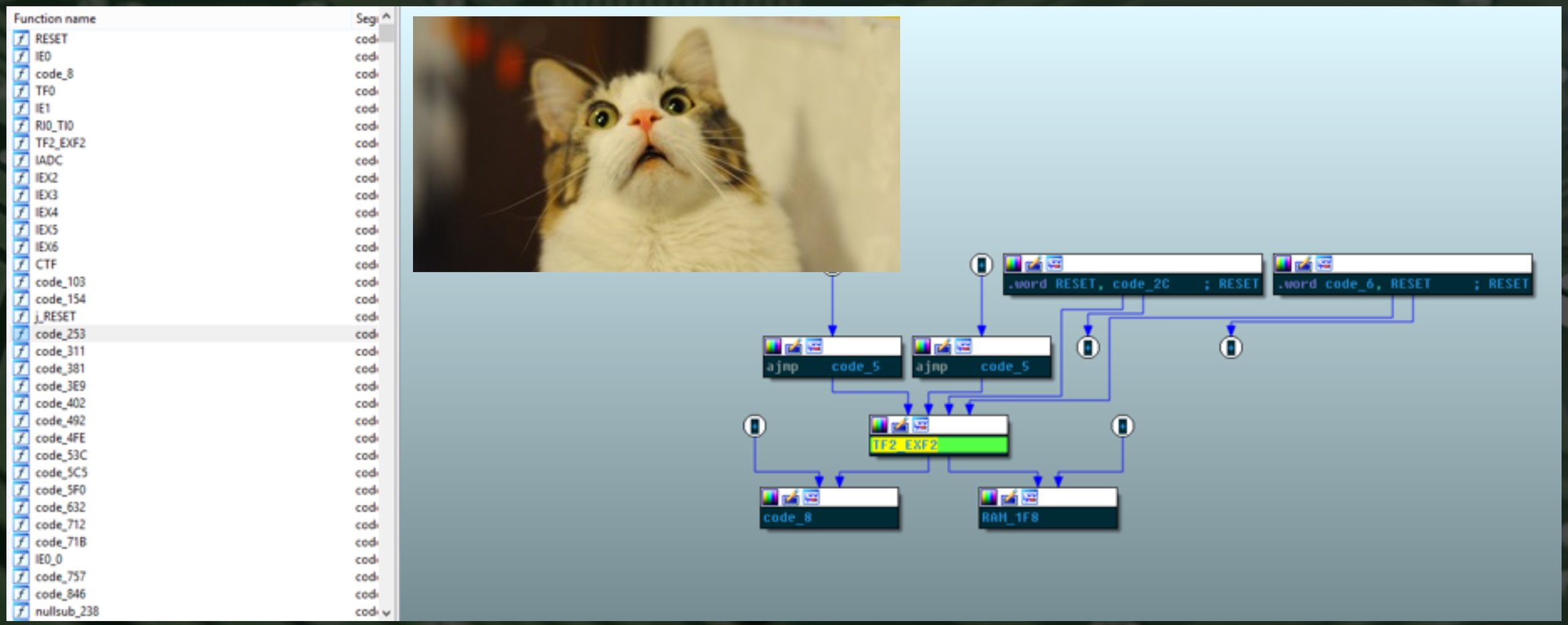


8051 ASSEMBLY?



8051 ASSEMBLY?

EVERYTHING IS 8051!!!



BREAKINGCODE

0000h:	9E	70	61	10	36	10	55	68	60	90	FF	10	4A	58	38	A4	žpa.6.Uh`.ÿ.JX8¤
0010h:	47	10	11	10	B5	B0	11	92	E5	11	11	10	DE	8F	11	91	G...µ°.'å...Þ..'
0020h:	F8	27	11	10	00	11	11	AF	FD	AB	7D	90	86	F9	16	1A	ø'.....¯ý«}.†ù..
0030h:	02	26	22	D0	90	03	AB	07	62	10	83	28	81	A2	87	16	.&"Ð..«.b.ƒ(.¢‡.
0040h:	00	EF	42	18	10	62	81	84	1D	07	07	83	10	B0	87	83	.ïB..b.„...ƒ.°‡ƒ
0050h:	83	10	B0	97	07	B8	84	1D	97	90	68	84	B0	07	83	12	ƒ.°—.¸„.—.h„°.ƒ.
0060h:	22	08	02	26	07	19	90	87	10	1D	D2	07	83	84	B8	07	"..&...‡..Ò.ƒ„¸.
0070h:	07	83	84	B8	E2	83	B8	10	B8	E2	83	68	84	1D	07	90	.ƒ„¸âƒ¸.¸âƒh„...
0080h:	07	22	90	02	26	12	19	10	83	10	B8	26	07	87	84	1D	."..&...ƒ.¸&.‡„.
0090h:	36	07	B8	84	B8	07	83	83	84	B8	07	83	68	10	1D	36	6.¸„¸.ƒƒ„¸.ƒh..6
00A0h:	26	07	19	90	02	90	12	22	07	83	84	C0	71	20	87	10	&.....".ƒ„Àq ‡.
00B0h:	C0	81	83	B8	84	1D	07	07	68	84	1D	07	83	83	10	C0	À.ƒ¸„...h„..ƒƒ.À
00C0h:	02	26	12	19	90	81	90	07	97	07	87	84	B0	22	40	83	.&.....—.‡„°"@ƒ
00D0h:	83	31	07	23	08	20	1D	84	1D	07	07	83	20	B8	E2	23	ƒ1.#. .„...ƒ ¸â#
00E0h:	36	07	D0	84	B8	08	83	83	83	70	07	23	08	20	1D	84	6.Ð„¸.ƒƒƒp.#. .„
00F0h:	1D	07	07	83	20	C0	81	23	27	AF	10	96	42	08	83	F9	...ƒ À.#'¯.–B.ƒù
0100h:	02	18	1E	AC	C0	2F	F9	10	C0	F2	16	7D	84	70	1D	2F	...¬À/ù.Àò.}„p./
0110h:	AB	1A	90	12	F6	F9	87	03	26	07	D0	90	02	AB	22	FF	«...öù‡.&.Ð..«"ÿ
0120h:	04	10	45	30	40	75	F9	1E	18	10	E7	01	27	98	C6	70	..E0@uù...ç.'˜Æp
0130h:	F9	25	87	53	2F	43	AB	21	A1	B0	14	2F	87	87	AF	AF	ù%‡S/C«!¡°./‡‡¯¯
0140h:	72	03	F7	1D	07	1C	07	18	03	AB	43	AB	1A	10	70	22	r.÷.....«C«..p"
0150h:	F9	87	02	26	2F	80	90	FF	45	38	D2	07	F7	84	C0	40	ù‡.&/€.ÿE8Ò.÷„À@
0160h:	E7	81	1E	98	C6	04	10	07	AF	14	B2	29	F9	29	A3	27	ç..˜Æ...¯.²)ù)£'
0170h:	AF	02	AF	1C	07	A1	C0	27	45	38	7D	F9	20	AF	0A	40	¯.¯..¡À'E8}ù ¯.@
0180h:	E7	A7	1E	99	C6	04	10	F2	90	AB	D2	87	04	84	C0	1A	ç§.™Æ..ò.«Ò‡.„À.
0190h:	02	26	22	A7	90	03	AB	90	07	AF	90	02	26	22	B6	0A	.&"§..«..¯..&"¶.
FF00h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FF10h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FF20h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FF30h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FF40h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FF50h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FF60h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FF70h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FF80h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FF90h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FFA0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FFB0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FFC0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FFD0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FFE0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
FFF0h:	00	00	00	00	00	00	00	00	B2	A1	A1	89	A9	00	92	91	.....²¡¡‰©.''
0000h:																	

Final 8 bytes are different.

A CLUE?

- What do these last 8 bytes mean?
- Is this a clue left for us by a mad embedded developer?

CHECKSUM?

- Maybe they are simply a checksum value?

B2 A1 A1 89 A9 00 92 91

~~CHKSUM - DD38F4E8~~

~~CRC32 - 479AE264~~

~~ADLER - A37EFB…~~

~~MD5 - 43C030C2…~~

FIRMWAREDIFFS!

- We have only analyzed a single firmware version.

Last 8 Bytes							
91	99	99	89	91	B2	99	00
B2	92	89	81	A1	99	A1	89
92	00	A1	A1	89	B2	89	91
91	92	A1	89	A1	A1	B2	00
B2	A1	A1	89	A9	00	92	91
A1	92	00	89	B1	91	A1	B9
92	00	A1	89	91	B2	A1	89
00	A1	92	91	C1	B2	A1	89
00	91	A1	B2	C9	89	A1	92

Byte	Count
A1	17
89	11
91	9
0	8
B1	8
92	8
99	4
B9	2
C1	1

FIRMWAREDIFFS!

- By listing the versions next to the bytes.

Last 8 Bytes								Firmware Version
91	99	99	89	91	B2	99	00	3.3.3.1.2
B2	92	89	81	A1	99	A1	89	4.1.4.0.1
92	00	A1	A1	89	B2	89	91	4.2.4.1.1
91	92	A1	89	A1	A1	B2	00	4.2.4.1.4
B2	A1	A1	89	A9	00	92	91	4.2.4.1.5
A1	92	00	89	B1	91	A1	B9	4.2.4.1.6
92	00	A1	89	91	B2	A1	89	4.2.4.1.7
00	A1	92	91	C1	B2	A1	89	4.2.4.1.8
00	91	A1	B2	C9	89	A1	92	4.2.4.1.9

A PATTERN?

- Maybe if we look at the binary values of these “patterns”.

Digit	Hex	Binary
1	0x89	10001001
2	0x91	10010001
3	0x99	10011001
4	0xA1	10100001
5	0xA9	10101001
6	0xB1	10110001
7	0xB9	10111001
8	0xC1	11000001
9	0xC9	11001001

CANYOUCOUNT?

- Why is this counter located in the middle?

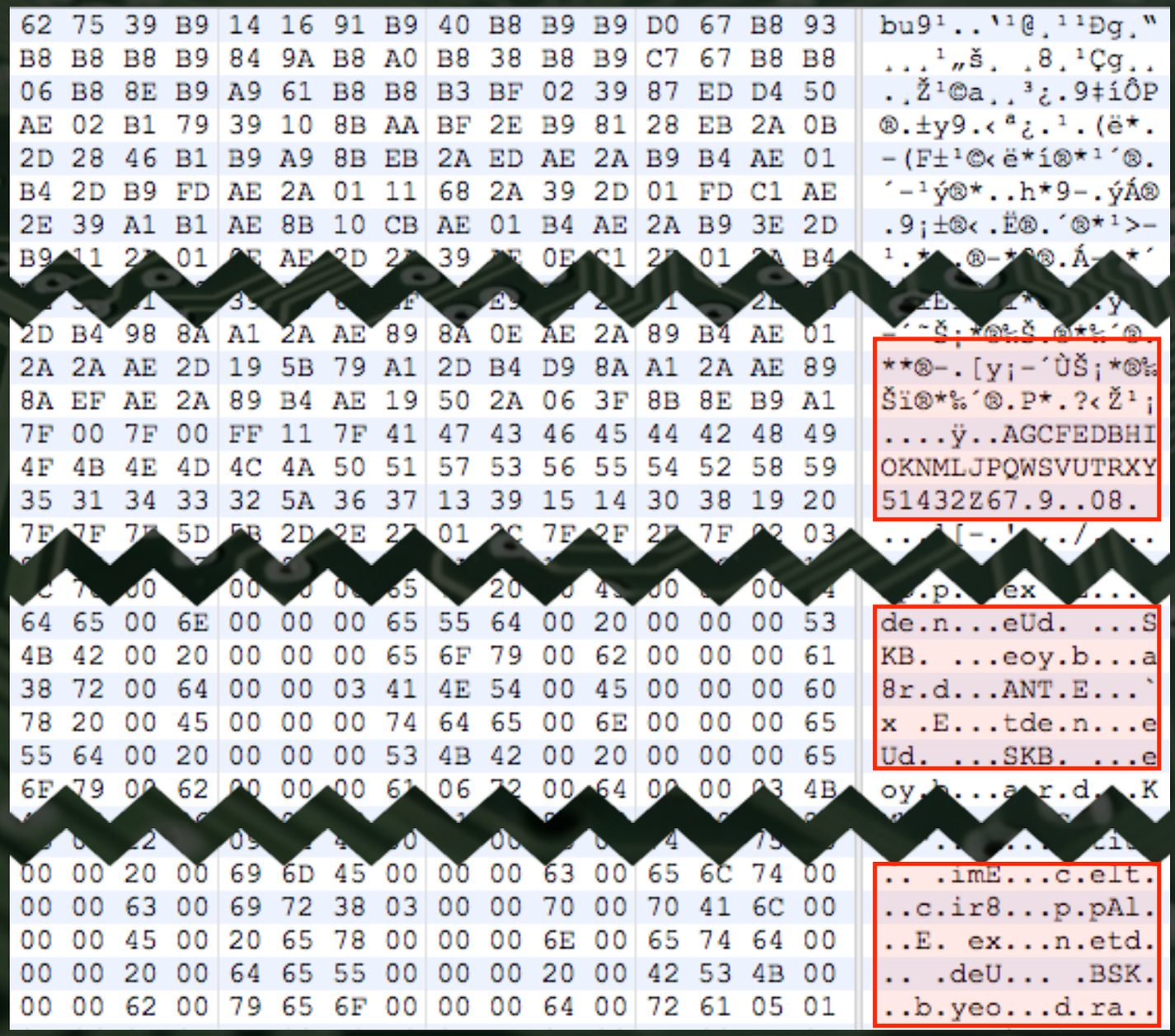
Digit	Hex	Binary	ROR 3	Hex
1	0x89	10001001	00110001	0x31
2	0x91	10010001	00110010	0x32
3	0x99	10011001	00110011	0x33
4	0xA1	10100001	00110100	0x34
5	0xA9	10101001	00110101	0x35
6	0xB1	10110001	00110110	0x36
7	0xB9	10111001	00110111	0x37
8	0xC1	11000001	00111000	0x38
9	0xC9	11001001	00111001	0x39

GOTIT?

- Just in case your ASCII-FU is lacking…

Digit	Hex	Binary	ROR 3	Hex	ASCII
1	0x89	10001001	00110001	0x31	“1”
2	0x91	10010001	00110010	0x32	“2”
3	0x99	10011001	00110011	0x33	“3”
4	0xA1	10100001	00110100	0x34	“4”
5	0xA9	10101001	00110101	0x35	“5”
6	0xB1	10110001	00110110	0x36	“6”
7	0xB9	10111001	00110111	0x37	“7”
8	0xC1	11000001	00111000	0x38	“8”
9	0xC9	11001001	00111001	0x39	“9”

STRINGS?



RESHUFFLE

1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8

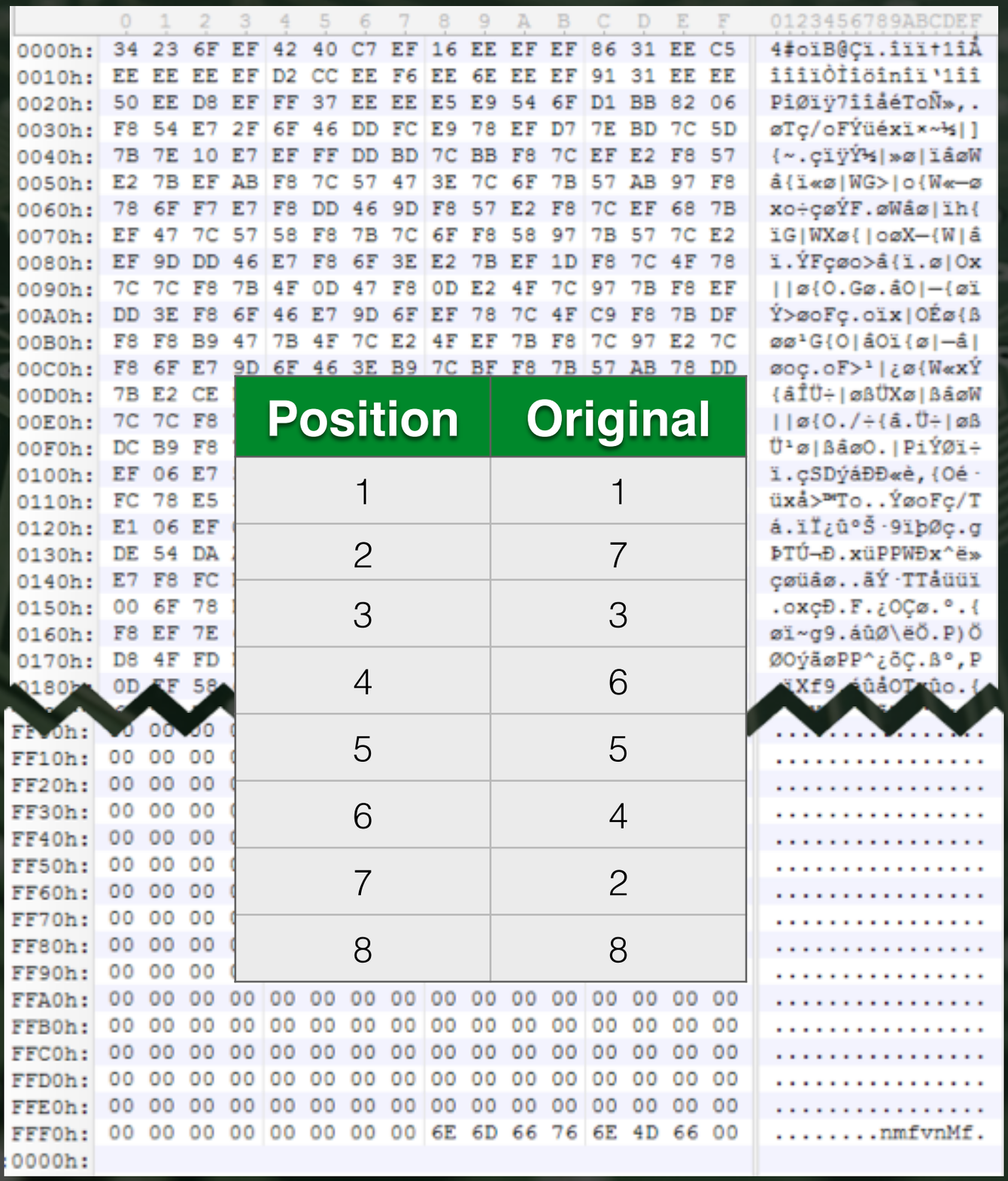
AGCFEDBHIOKNMLJPQWSVUTRX

ABCDEFGHIJKLMNOPQRSTUVWX

1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8

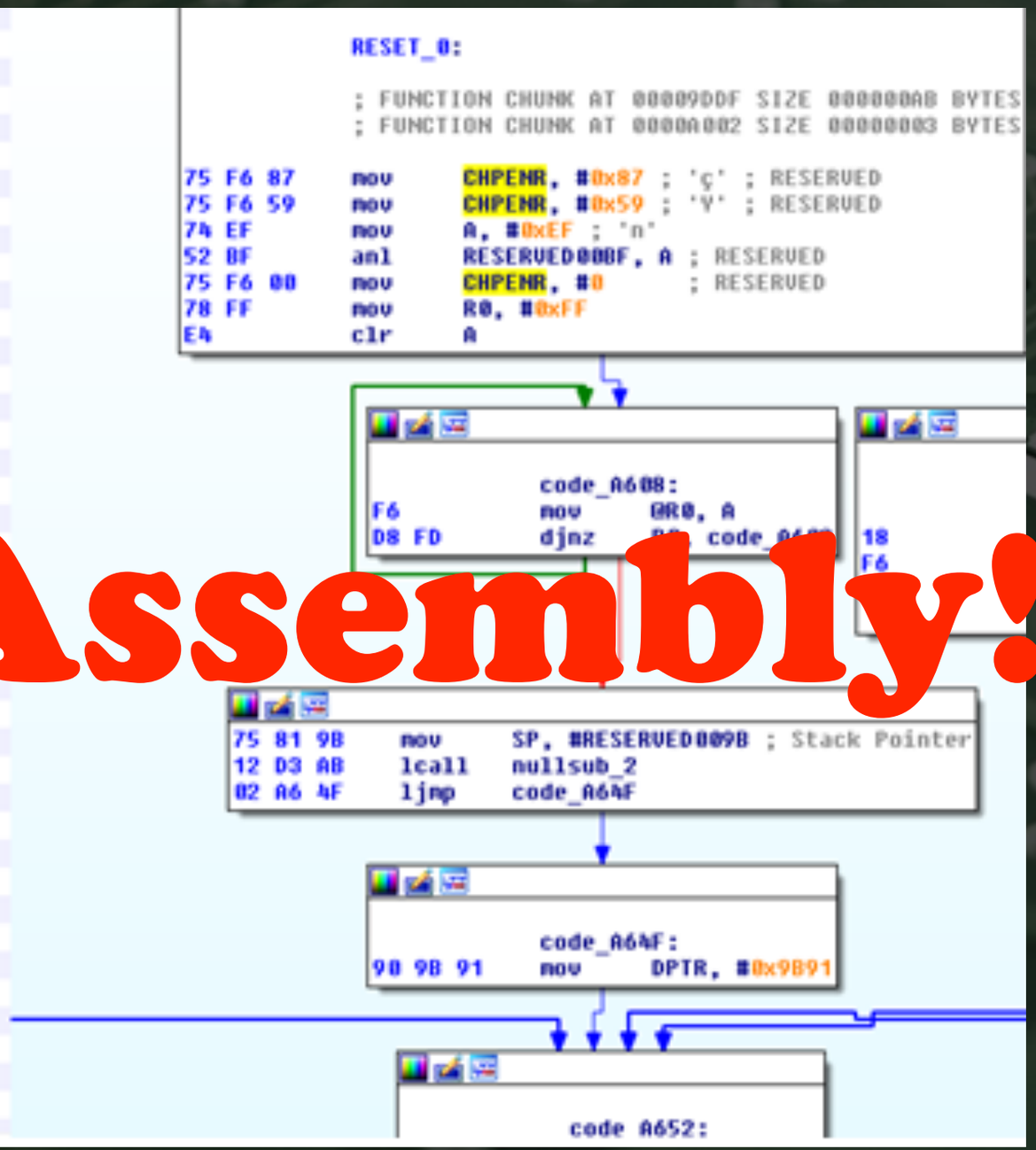
Position	Original
1	1
2	7
3	3
4	6
5	5
6	4
7	2
8	8

RESHUFFLE



Position	Original
1	1
2	7
3	3
4	6
5	5
6	4
7	2
8	8

SUCCESS!!!



Assembly!

8051FUN

- We can now design our own custom firmware.
- However, we do need a basic understanding of 8051 assembly!

8051REVIEW

+ Only 255 OP-Codes, and ~40 Instructions.

- Functions are not *really* functions.

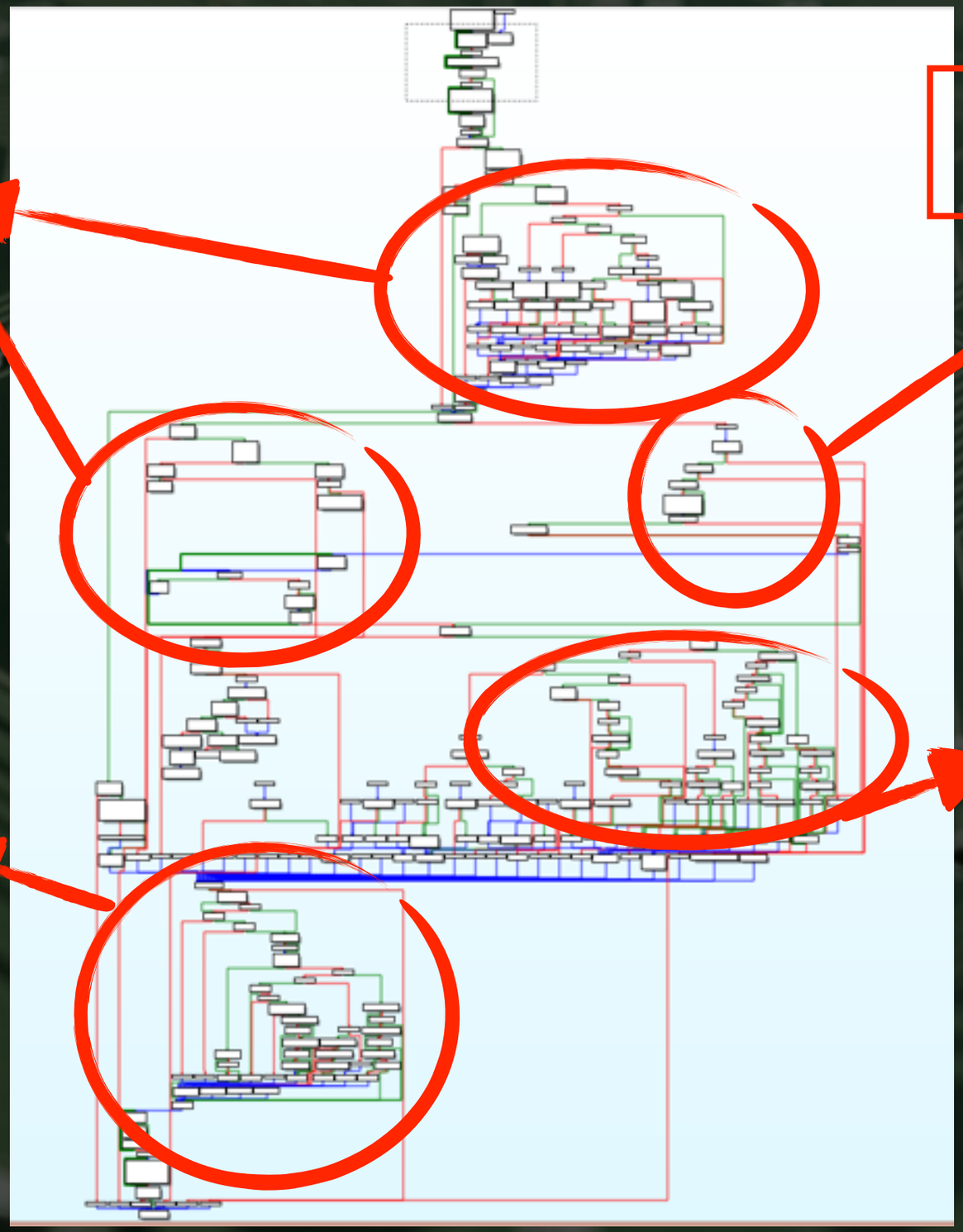
- Just a single memory access register.

- Registers keep on changing for some reason.

KVMLOGIC

Keyboard Emulation

HID Parsing



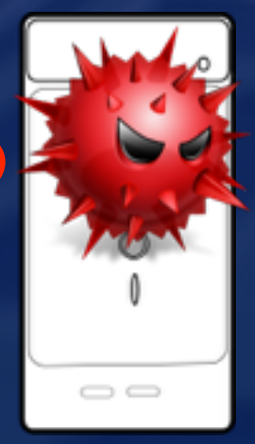
Keyboard LEDs Control

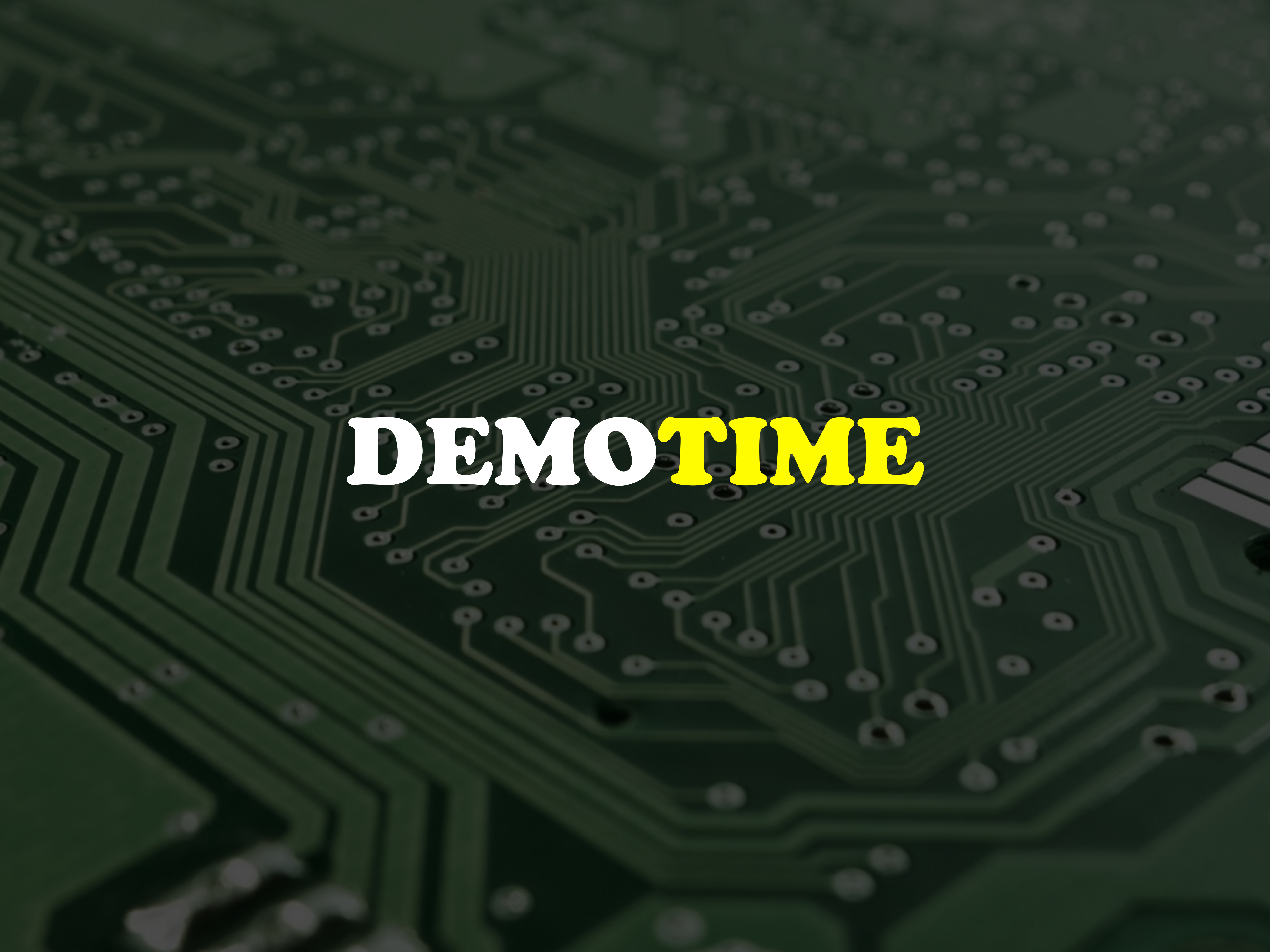
Hotkeys Handling

“HELLOKVM!”

Air Gapped Network

Internet Connected Network




DEMOTIME

ATTACK VECTORS

- Yes, we had physical access to the device.
  - Just get 30 seconds alone with a KVM. (“evil maid”)
  - Supply chain attack (“Interdiction”).
- Many KVMs update over IP.
- KVMs are not exploit proof.

COUNTERMEASURES

- Know your environment.
- Secure your KVMs.
- Be innovative!

Thank You!

@ynvb
@oppenheim1