

Key-Logger, Video, Mouse

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



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

MEET THE TEAM



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

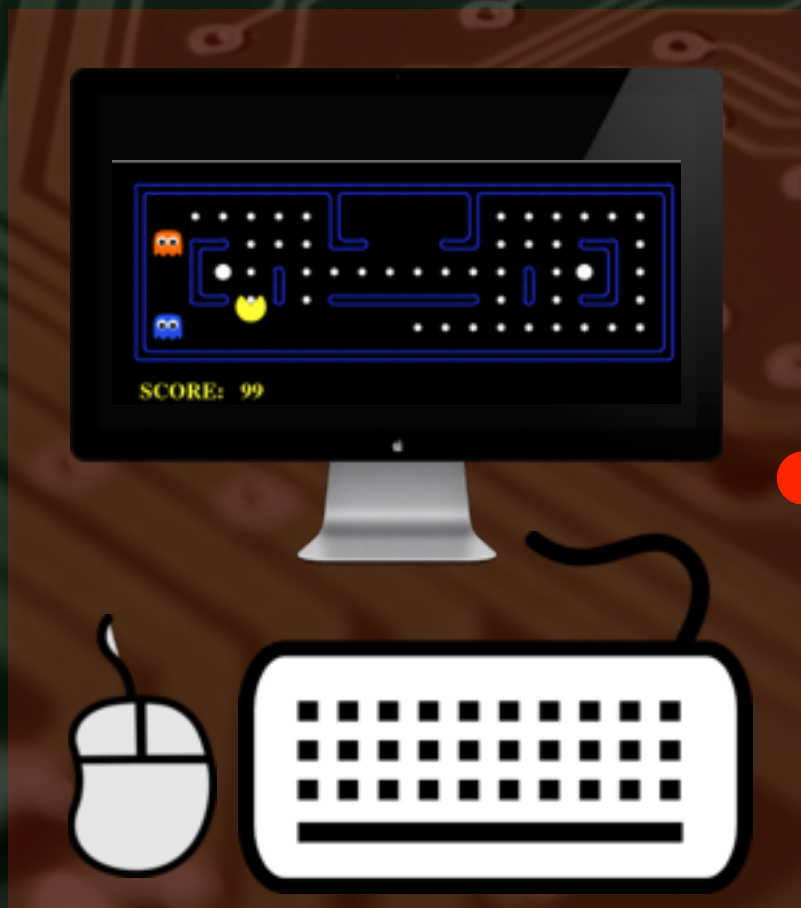
TOOMANYCOMPUTERS

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



WHAT IS KVM?

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



KVM

1

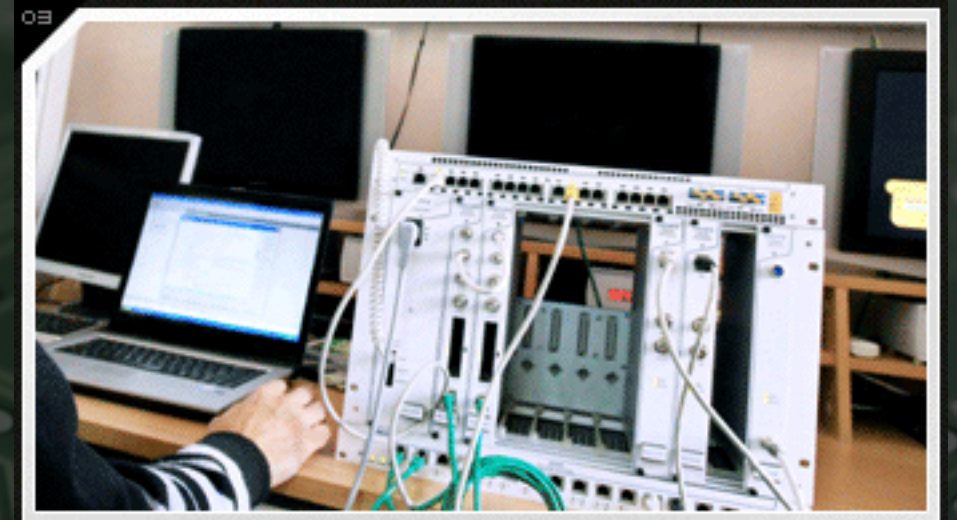
2



WHERE ARE THEY?

- 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

STUPID BOXES?

NTI Main Menu

Name	Type	Stat
2 PORT 02	USB	OFF 1
3 PORT 03	USB	
4 PORT 04	USB	
5 PORT 05	USB	
6 PORT 06	USB	
7 PORT 07	USB	
8 PORT 08	USB	
9 PORT 09	USB	

Admin Settings List
Scan=N BCast=N Find

Administration Menu

Choose Admin Function

- 1 System Configuration
- 2 User Configuration
- 3 Channel Configuration
- 4 User Station Profile
- 5 System Reboot
- 6 System Reset Settings
- 7 Network Setting

Edit FKey Esc
ScrLock | Scan

ALTUSCN Enterprise Solutions by ATEN

Port Number	Port Name	Device Name	Status	Operation
[04-04]				
1		KH1500A	Online	Connect
2		KH1500A	Online	Connect
3		KH1500A	Online	Connect
4		KH1500A	Online	Connect
5		KH1500A	Offline	Connect
6		KH1500A	Offline	Connect
7		KH1500A	Offline	Connect
8		KH1500A	Offline	Connect

Copyright © 2009-2012 ATEN International Co., Ltd.

IT RUNS CODE!!

WHAT CAN WE DO?

- 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!

MEET THE BLOB

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 F6 F3 42 C1 B6 42 42 43 8D DC 42 C2	CBC*ãRÁqBRC ÜBÂ
0020h:	AB 74 42 43 53 42 42 FC AE F8 2E C3 D5 AA 45 49	<tBCSBBU@e.Ã*EI
0030h:	51 75 71 83 C3 58 54 31 43 D0 7F 02 F1 00	QuqfÃPøT1C@ (ñÔE
0040h:	53 BC 11 4B 43 52 54 54 D3 54 54 54 54 54 54	S*.KC10*NTT@C&ÔD
0050h:	D0 43 E3 C4 53 53 C3 3B D3 53 53 53 53 53 53	ÐC&ÂTe*NAA; *TÐA
0060h:	71 5B 51 75 54 4A C3 D4 43 4E 81 54 D0 D7 EB 54	q[QuTJÃÖCN. T@*eT
0070h:	54 00 D7 5B 51 00 5B 53 5B 51 00 5B D7 4E 54 C3	QvY@P@C@T@NTÃ
0080h:	54 71 C3 51 75 41 4A 43 D0 43 EB 75 54 D4 D7 4E	TqÃQuAJC@CeuTÔ*N
0090h:	65 54 EB D7 EB 54 D0 D0 D0 54 D0 3B 43 4E 65	eT@*eTÐÐ*eTÐ/ CNe
00A0h:	75 54 4A C3 51 51 51 51 51 51 51 51 51 51 51	vJÃQÃAqT@*""sÔC
00B0h:	93 D2 D0 53 53 53 53 53 53 53 53 53 53 53 53	Ð@e*NIT; *NT@ÐC"
00C0h:	51 75 41 4A C3 D2 C3 54 C4 54 D4 D7 E3 71 13 D0	QuAJÃÖATATÔ*q.Ð
00D0h:	D0 53 54 70 5B 73 4E D7 4E 54 54 D0 73 5B 51 70	Ð@P[anXNTT@P@eip
00E0h:	65 54 83 D7 EB 5B D0 D0 D0 23 54 70 5B 73 4E D7	eTf*e[ÐÐÐ#T@]sN*
00F0h:	4E 54 54 D0 53 D2 70 53 43 C3 11 5B D0 5A	NTT@e"ÔptúCÃ [Ð*
0100h:	51 4B 4D FF 5A 43 5A 43 5A 43 5A 43 5A 43 5A 43	QKMy" "C";E. #N
0110h:	F8 49 C3 41 5A 50 5A 50 5A 50 5A 50 5A 50 5A 50	eIÃAV*ÔPuTfÃ@øq-
0120h:	57 43 16 63 13 26 AA 4D 4B 43 B4 52 74 C@ 53 23	WC.c. &*MKC' R@E*#
0130h:	AA 76 D4 00 7C 10 5B 72 E2 53 47 7C D4 D4 5C 5C	!vÔ .er&GLOûú
0140h:	21 50 A4 4E 54 4F 54 4B 50 F8 10 F8 49 43 23 71	!P=NTOTKP@.e@C#q
0150h:	AA 54 51 75 7C D3 53 AC 16 6B 81 54 A4 D7 93 13	*ÔQu ÔÃ-k.T@*".
0160h:	B4 51 51 51 51 51 51 51 51 51 51 51 51 51 51	z@t
0170h:	FC 51 FC 4F 54 F2 93 74 16 6B 2E AA 73 5C 59 13	uQuT@-c.kI.*üY.
0180h:	B4 F4 4D CA 95 57 43 A1 C3 F8 81 D4 57 D7 93 49	'ÔMÊ*WC;Ã@.Ôv*"I
0190h:	51 75 71 F4 C3 50 5B C3 54 FC C3 51 75 71 E5 59	QuqoAP@ATuAQuqâY
FF00h:	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	SSSSSSSSSSSSSSSS
FF20h:	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	SSSSSSSSSSSSSSSS
FF40h:	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	SSSSSSSSSSSSSSSS
FF60h:	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	SSSSSSSSSSSSSSSS
FF80h:	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	SSSSSSSSSSSSSSSS
FFA0h:	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	SSSSSSSSSSSSSSSS
FFC0h:	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	SSSSSSSSSSSSSSSS
FFE0h:	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	SSSSSSSSáòòÚúSÃÃ
0000h:		

Size - 64K

Low Entropy

No Strings

Inconclusive freq. analysis

binwalk





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.

PROTOCOL ANALYSIS

Handshake

Data Transfer

46 55 90 00 44 49 <u>b8</u>	FUê.DIΠ
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 <u>34</u>	2A..MAIN...V42R4
31 37 56 31 30 52 30 38 31 57 37 38 45 36 35 00	17V10R081W78E65.
00 <u>a2</u>	.ç
46 55 <u>a0 00</u> 43 54 <u>d2</u>	FU†.CT“
46 55 <u>20 00</u> 00 <u>bb</u>	FU_.. ^a
46 55 <u>a2 00</u> ** ** ** ** ** ** ** ** ** 2d 31 37 33 ** 41	FUç.*****-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.™..âisI.¿j«.¨
7f 25 25 49 <u>10</u>	%I_.
46 55 <u>22 00</u> 00 <u>bd</u>	FU"_.Ω
46 55 <u>a3 00</u> <u>00 00</u> 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.-...Σÿv..z.
04 84 e3 17 04 05 04 04 04 ba 15 ed 32 05 ec 68	.Ñ,,.....f.Ì2.Ïh
03 0f 8b 0f be 85 16 37 be 12 85 07 13 c5 b7 96	..ã.æÖ.7æ.Ö..≈Σñ
92 03 94 7f 05 3d <u>2a</u>	í.î.=*



46 55 <u>a3 00</u> <u>03 63</u> 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÷ÂfIU¶'".÷Ö.'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	fI'Â¶U÷¶.-'Ö"'÷ñö
a5 01 40 85 d7 d7 <u>81</u>	•.@Ö♦♦Ä
46 55 <u>23 00</u> <u>03 63</u> 00 <u>24</u>	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	.CBCæãBÁqBBC.ÜBÃ
0020h:	AB 74 42 43 53 42 42 FC AE F8 2E C3 D5 AA 45 49	«tBCSBBÜ®.ÃÕ*EI
0030h:	51 75 71 83 C3 50 F8 54 31 43 D0 7B D2 F1 D4 45	QuqfÃPøT1CÐ(ÔñÔE
0040h:	53 BC 11 4B 43 31 D2 D7 4E 54 54 D0 43 E3 D4 D0	S4.KC1Ò*NTTÐCãÔÐ
0050h:	D0 43 E3 C4 54 EB D7 4E C4 C3 3B D7 E3 54 D0 41	ÐCãÄTe*NÃÃ; *ãTÐA
0060h:	71 5B 51 75 54 4A C3 D4 43 4E 81 54 D0 D7 EB 54	q[QuTJÃÖCN.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	"ÔÐë*NTT; *NTÐÐC"
00C0h:	51 75 41 4A C3 D2 C3 54 C4 54 D4 D7 E3 71 13 D0	QuAJÃÖÃTÃTÔ*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	eTf*ë[ÐÐÐ#Tp[sN*
00F0h:	4E 54 54 D0 73 93 D2 70 74 FC 43 C5 11 5B D0 AA	NTTÐs"ÔptüCÃ. [Ð*
0100h:	51 4B 4D FF 93 7C AA 43 93 A1 45 2E D7 23 4E 7C	QKMÿ" °C"; E. *#N
0110h:	F8 49 C3 41 A5 AA D4 50 75 54 83 C3 51 F8 71 AC	øIÃA#*ÔPuTfÃQøq-
0120h:	57 43 16 63 13 26 AA 4D 4B 43 B4 52 74 CB 95 23	WC.c. & *MKC' RtE*#
0130h:	AA 76 D4 00 7C 10 F8 72 F2 E3 47 7C D4 D4 FC FC	*vÔ. .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	*ÔQu ÓÃ-.k.T#*".
0160h:	B4 D2 4D CB 95 57 43 54 FC 47 E1 7A AA 7A F0 74	'ÔMË*WCTüGáz* zøt
0170h:	FC 51 FC 4F 54 F2 93 74 16 6B 2E AA 73 FC 59 13	üQuÔTò"t.k.*süY.
0180h:	B4 F4 4D CA 95 57 43 A1 C3 F8 81 D4 57 D7 93 49	'ÔMË*WC;Ãø.ÔW*"I
0190h:	51 75 71 F4 C3 50 F8 C3 54 FC C3 51 75 71 E5 59	QuqôÃPøÃTüÃQuqãY
FF00h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF10h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF20h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF30h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF40h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF50h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF60h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF70h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF80h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF90h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFA0h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFB0h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFC0h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFD0h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFE0h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFF0h:	53 53 53 53 53 53 53 53 E1 F2 F2 DA FA 53 C1 C2	SSSSSSSSáòòÚúSÃÃ
0000h:		



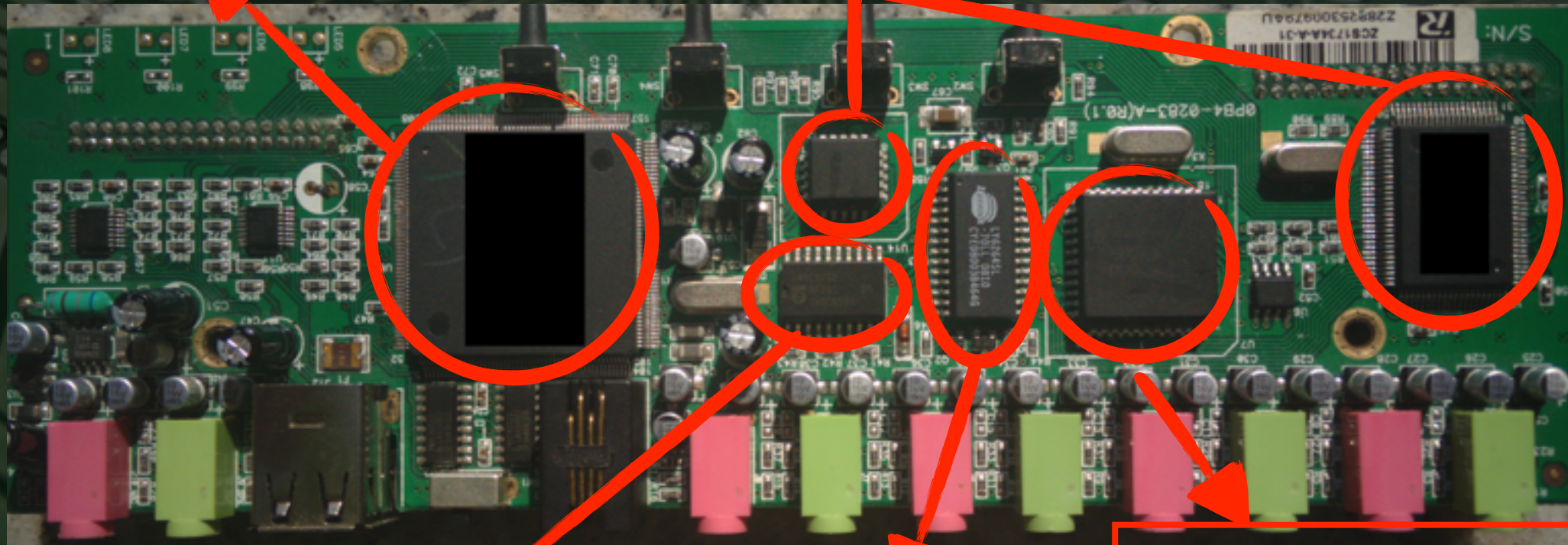


FAIL!

PCB LAYOUT

Unknown

PLD

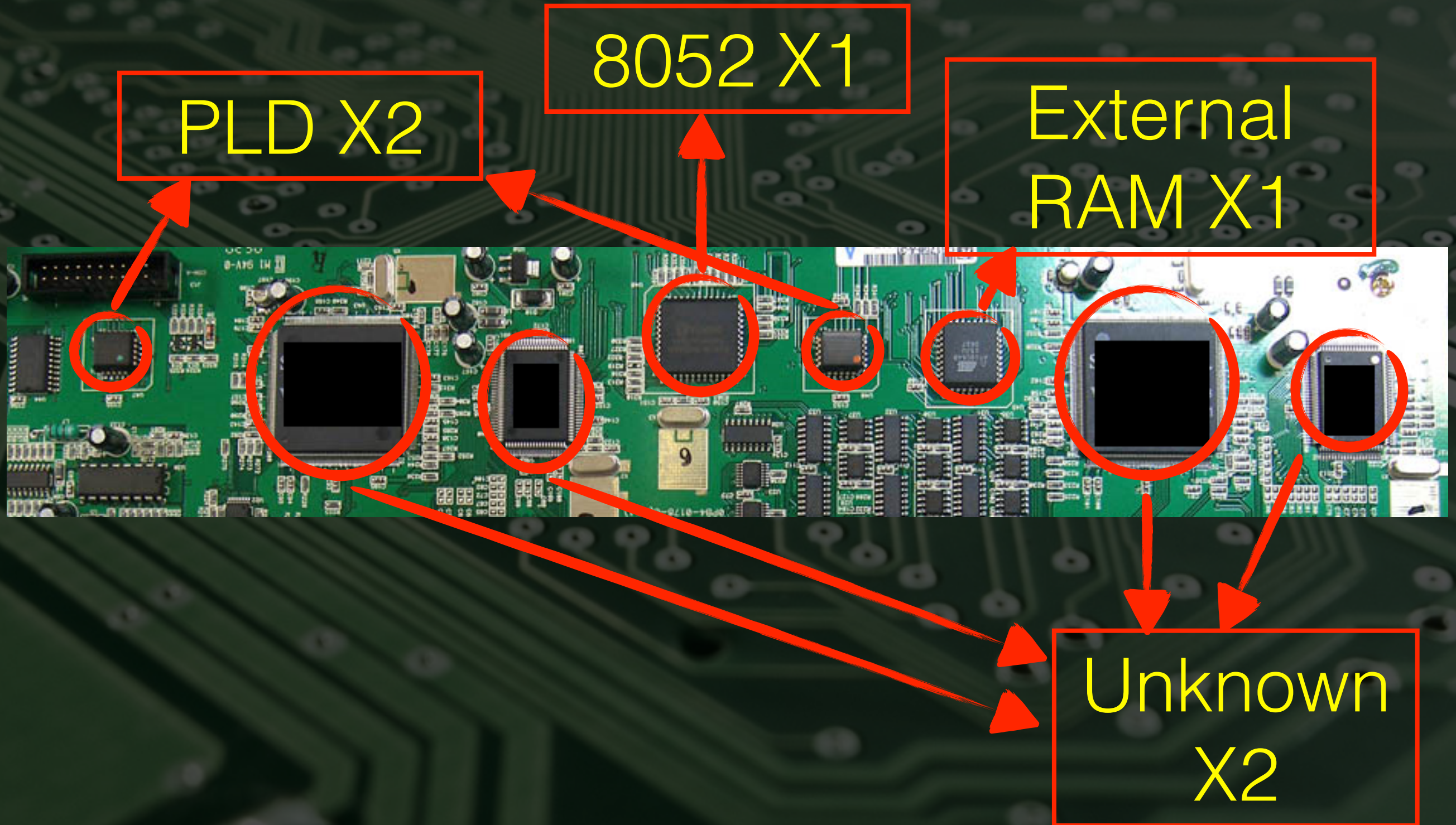


D-Latch

2K
External
RAM

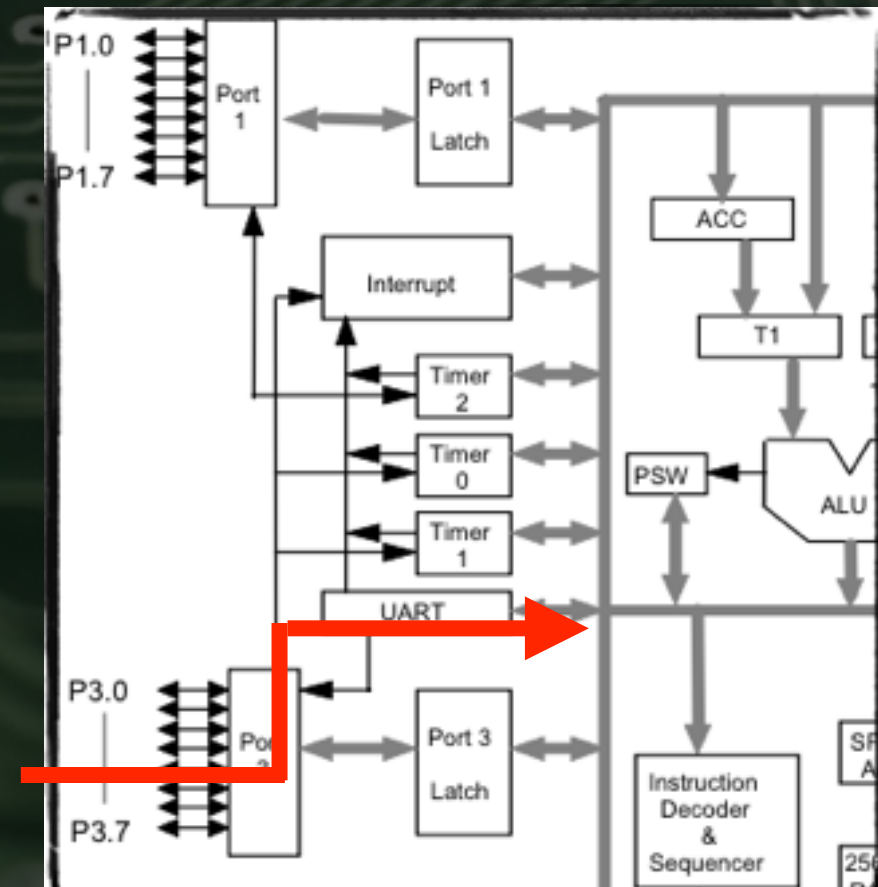
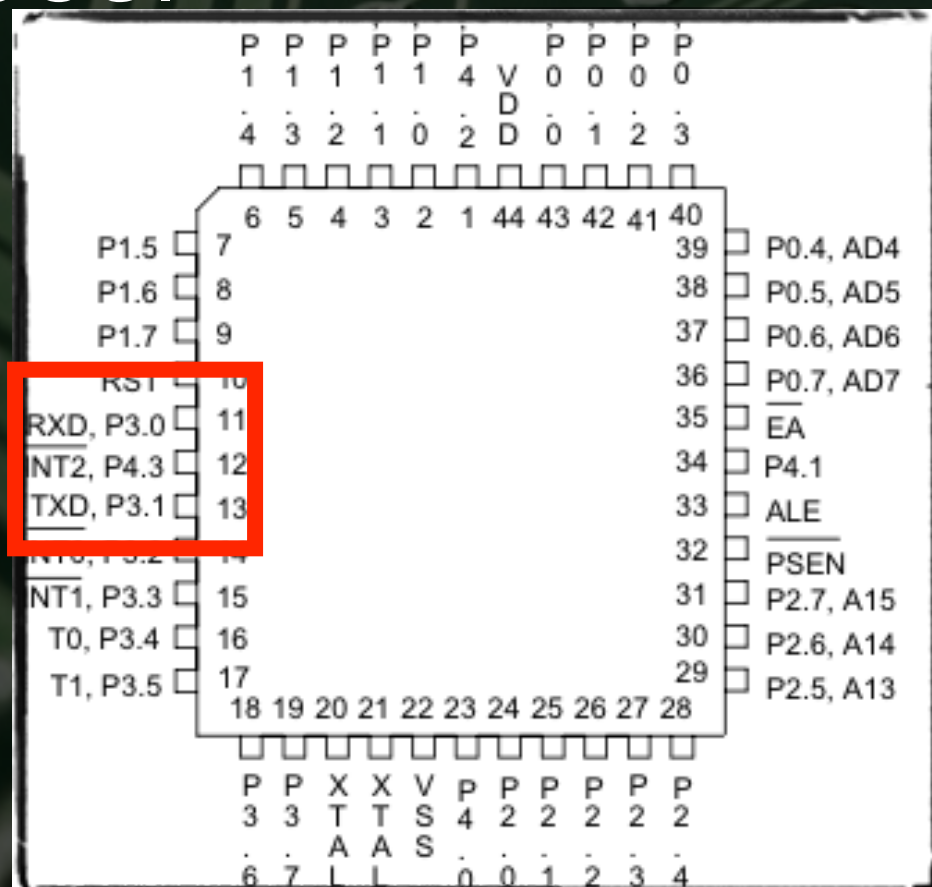
8052
Processor

PCBLAYOUT



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.



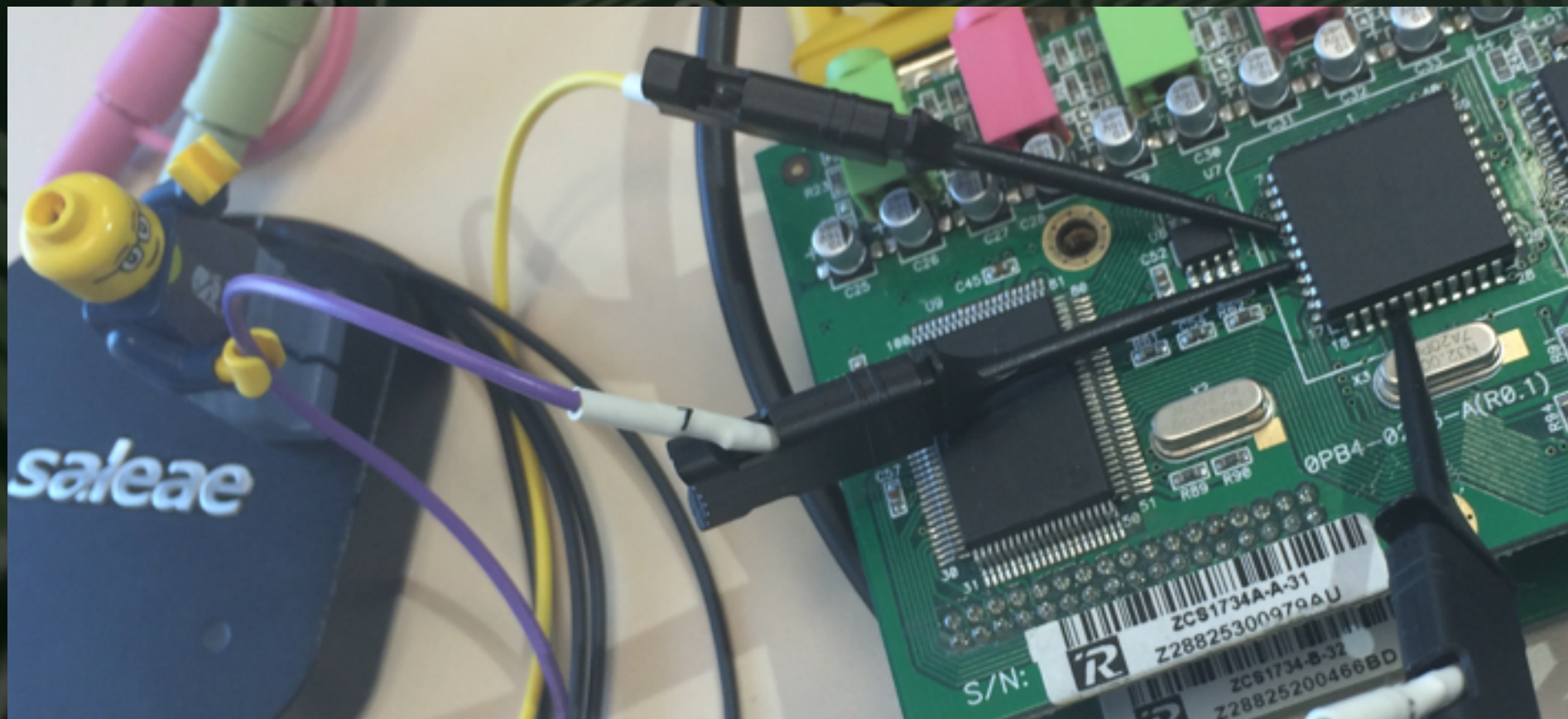
NOTHING **BUT** LOGIC

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



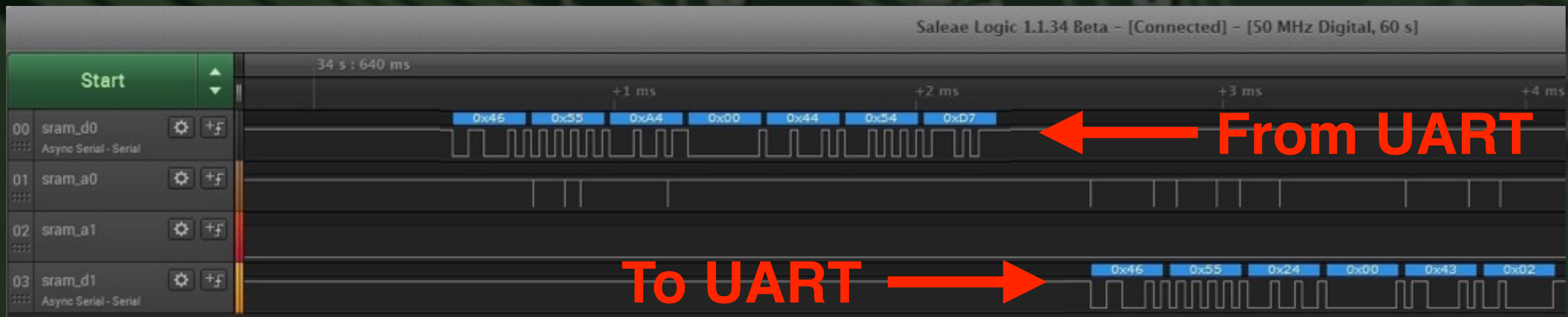
TAPICPINS

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



SIGNAL ANALYSIS

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



GREAT FAIL!

46 55 90 00 44 49 b8	FUê.DIÏ
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.Æ.βuP5 ™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	FU" ..Ω
46 55 a3 00 00 00 05 60 70 7d 5b a7 65 05 7d ca	FU£...hp}[0e.MÍ
2d a1 4f 55 85 05 d1 04 04 b7 d8 76 05 05 7a 04	-°OUÖ.-..Σÿv..z.
04 84 e3 17 04 05 04 04 04 ba 15 ed 32 05 ec 68	.Ñ,,.....f.Ì2.Ïh
03 0f 8b 0f be 85 16 37 be 12 85 07 13 c5 b7 96	..ã.æÖ.7æ.Ö..≈Σñ
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÷ÂfU¶'".÷Ö.'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÷¶.-'Ö"'÷ñÖ
a5 01 40 85 d7 d7 81	•.@Ö♦♦Å
46 55 23 00 03 63 00 24	FU#..c.\$

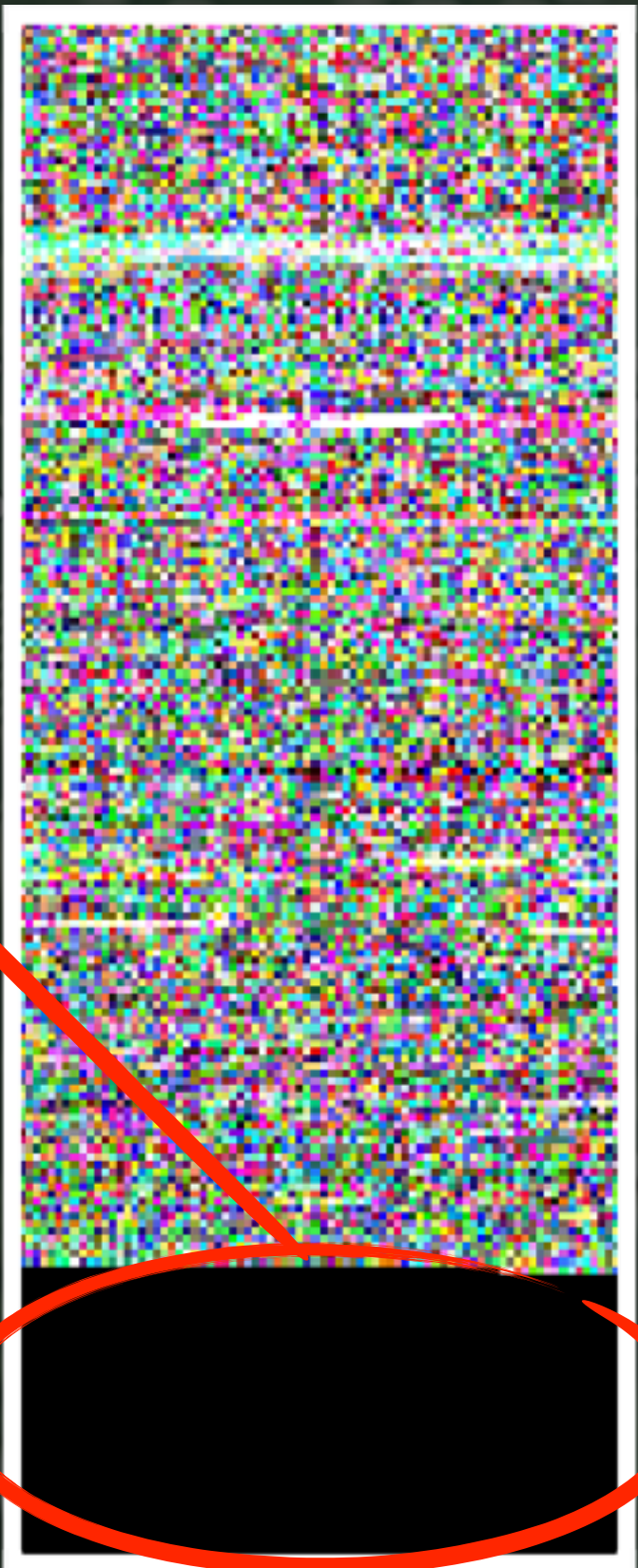
BREAKING **CODE**

- 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!

REMEET THE BLOB

0000h:	CD 23 32 43 65 43 06 3B 33 C3 AC 43 19 0B 6B F7	í#2CeC.;3Ä-C..k+
0010h:	14 43 42 43 E6 E3 42 C1 B6 42 42 43 8D DC 42 C2	.CBCeãBÄqBBCC ÜBÄ
0020h:	AB 74 42 43 53 42 42 FC AE F8 2E C3 D5 AA 45 49	<tBCSBBU@e.Ä@*EI
0030h:	51 75 71 82 C3 50 54 53 43 D0 7B D2 F1 D4 45	QcçãPæT1C@{(ñÖE
0040h:	53 BC 11 43 42 D3 43 44 43 44 43 44 43 44 43	SÄ@LÖ*NTT@CÄÖD
0050h:	D0 43 43 43 43 43 43 43 43 43 43 43 43 43	ðC@Te*NÄÄ;*T@A
0060h:	71 5B 51 75 54 4A C3 D4 43 4E 81 54 D0 D7 EB 54	q[QuTJÄÖCN.T@*eT
0070h:	54 D0 D7 EB B1 43 EB 43 B B1 D0 43 4E 54	T@*eT;NTÄ
0080h:	53 BC 11 43 42 D3 43 44 43 44 43 44 43 44	SÄ@LÖ*NTT@CÄÖD
0090h:	53 BC 11 43 42 D3 43 44 43 44 43 44 43 44	SÄ@LÖ*NTT@CÄÖD
00A0h:	5 54 4A C3 51 C3 41 71 54 D0 D7 93 22 73 D4 43	uTJÄQÄÄqT@*sÖC
00B0h:	93 D2 D0 EB D7 4E 54 54 3B D7 4E 54 D0 D0 43 93	"ÖD@*NTT;*NTT@C"
00C0h:	51 75 41 4A C3 D2 C3 54 C4 54 D4 D4 E3 71	QuAJÄÖÄTÄTÖ*Äq.ð
00D0h:	D0 62 54 70 5B 73 4E D7 4E 54 54 73 EB	ðbTp[sN*NTT@seip
00E0h:	65 54 83 D7 EB 5B D0 D0 D0 23 54 70 5B 73 4E D7	eTf*ë[ððð#Tp[sN*
00F0h:	4E 54 54 D0 73 93 D2 70 74 FC 43 05 11 5B D0 AA	NTT@S"ÖptüCÄ. [ð*
0100h:	51 4B 4D FF 93 7C AA 43 93 A1 45 E D7 23 4E 7C	QÄMÿ" *C";E.*#N
0110h:	F8 49 C3 41 A5 AA D4 50 75 54 83 C3 51 F8 71 AC	øIAÄ#*ÖPuTfÄQøq-
0120h:	57 43 16 63 13 26 AA 4D 4B 43 B4 52 74 CB 95 23	WC.c.*MKC'RtE*#
0130h:	AA 76 D4 00 7C 10 F8 72 F2 E3 47 7C D4 D4 FC FC	*vö. .ø.ðAG ÖÖüü
0140h:	21 50 A4 4E 54 4F 54 4B 50 F8 1 F8 49 43 23 71	!P=NTOTKÄ.øIC#q
0150h:	AA D4 51 75 7C D3 C3 AC 16 6B 8 54 A4 D7 93 13	*ÖQu ÖÄ-.k.ø*"
0160h:	B4 D2 4D CB 95 57 43 54 FC 47 7A AA 7A F0 74	'ÖMË*WCTÜGáz-Ät
0170h:	FC 51 FC 4F 54 F2 93 74 16 6B E AA 73 FC 59 13	üQuÖTò"t.k.*sü
0180h:	B4 F4 4D CA 95 57 43 A1 C3 F8 51 D4 57 D7 93 49	'ÖMË*WC;Äø.ÖW*"I
0190h:	51 75 71 F4 C3 50 F8 C3 54 FC C3 51 75 71 E5 59	QuqöÄPæÄTüÄCuqäY
FF00h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF10h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF20h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF30h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF40h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF50h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF60h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF70h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF80h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FF90h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFA0h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFB0h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFC0h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFD0h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFE0h:	53 53 53 53 53 53 53 53 53 53 53 53 53 53	SSSSSSSSSSSSSSSSSS
FFF0h:	53 53 53 53 53 53 53 53 E1 F2 F2 DA FA 53 C1 C2	SSSSSSSSáòòÜúSÄÄ
0000h:		

Last Bytes are padded with 0x53



ALL DONE!

0000h:	9E 70 61 10 36 10 55 68 60 90 FF 10 4A 58 38 A4	žpa.6.Uh`.ý.JX8µ
0010h:	47 10 11 10 B5 B0 11 92 E5 11 11 10 DE 8F 11 91	G...µ°.á...p..`
0020h:	F8 27 11 10 00 11 11 AF FD AB 7D 90 86 F9 16 1A	ø'.....ý«).tù..
0030h:	02 26 22 D0 90 03 AB 07 62 10 83 28 81 A2 87 16	.&"Đ..«.b.f(.e†.
0040h:	00 EF 42 18 10 62 81 84 1D 07 07 83 10 B0 87 83	.iB..b.....f.°†f
0050h:	83 10 B0 97 07 B8 84 1D 97 90 68 84 B0 07 83 12	f.°-.,,,-.h,,°.f.
0060h:	22 08 02 26 07 19 90 87 10 1D D2 07 83 84 B8 07	"..&...†..ò.f,,.
0070h:	07 83 84 B8 E2 83 B8 10 B8 E2 83 68 84 1D 07 90	.f,,.âf,,.âfh,,...
0080h:	07 22 90 02 26 12 19 10 83 10 B8 26 07 87 84 1D	."..&...f.,&.†,,.
0090h:	36 07 B8 84 B8 07 83 83 84 B8 07 83 68 10 1D 36	6.,,,.ff,,.fh..6
00A0h:	26 07 19 90 02 90 12 22 07 83 84 C0 71 20 87 10	&.....".f,,.Àq †.
00B0h:	C0 81 83 B8 84 1D 07 07 68 84 1D 07 83 83 10 C0	À.f,,...h,,.ff.À
00C0h:	02 26 12 19 90 81 90 07 97 07 87 84 B0 22 40 83	.&.....-†,,.°@f
00D0h:	83 31 07 23 08 20 1D 84 1D 07 07 83 20 B8 E2 23	f1.#.f ,â#
00E0h:	36 07 D0 84 B8 08 83 83 83 70 07 23 08 20 1D 84	6.Đ,,.ffffp.#. ..
00F0h:	1D 07 07 83 20 C0 81 23 27 AF 10 96 42 08 83 F9	...f À.#'-.B.fù
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†.&.Đ..«"ÿ
0120h:	04 10 45 30 40 75 F9 1E 18 10 E7 01 27 98 C6 70	..E0@uù...ç.'~Ep
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..~E...~.°)ù)é'
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	çS.™E..ò.«ò†..„À.
0190h:	02 26 22 A7 90 03 AB 90 07 AF 90 02 26 22 B6 0A	.ç"S...~.ç"ÿ.
FF00h:	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
FF20h:	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
FF40h:	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
FF60h:	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
FF80h:	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
FFA0h:	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
FFC0h:	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
FFE0h:	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°;i;«@.'`
0000h:		



8051 ASSEMBLY?

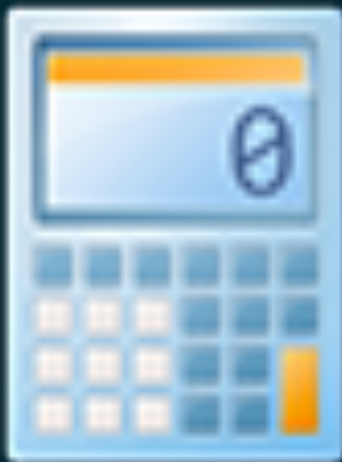
Function name	Seg
RESET	code
IE0	code
TF0	code
IE1	code
TF1	code
TF2_EXF2	code
IADC	code
IEX2	code
IEX3	code
IEX4	code
IEX5	code
IEX6	code
RI1_TI1	code
code_454	code
code_B7B	code
code_ECE	code
code_EDD	code
code_EFB	code
code_F6F	code
code_14D7	code
code_1678	code
code_167B	code
code_195A	code
code_196F	code
code_1B07	code
code_1C14	code
code_1C6F	code
code_1CFF	code
code_1D6F	code
code_1E6F	code
code_1ED1	code
code_24B7	code
code_286F	code
code_2B50	code
code_2E78	code
code_2EDC	code
code_2F78	code
code_30C6	code
code_3156	code
code_365E	code

```
code:00000003
code:00000003 ; External interrupt 0
code:00000003
code:00000003 ; public IE0
code:00000003 IE0: ; CODE XREF: RI1_TI1+3C76↓p
code:00000003 xrl A, R7
code:00000004 xch A, R1
code:00000005 mov ARCON, #0xCB ; '-' ; Arithmetic Control Register
code:00000008 mov A, R6
code:00000009 djnz R6, 0xFFFF9
code:00000009 ; End of function IE0
code:00000009
code:0000000B ; ===== S U B R O U T I N E =====
code:0000000B ; Timer 0 overflow
code:0000000B
code:0000000B ; public TF0
code:0000000B TF0:
code:0000000B mov A, R7
code:0000000C addc A, @R0
code:0000000D inc R4
code:0000000E mov A, R7
code:0000000F mov R5, MD5 ; Multiplication/Division Register 5
code:00000011 code_11: ; CODE XREF: code:00000027↓j
code:00000011 mov MD5, R7 ; Multiplication/Division Register 5
code:00000011 ; End of function TF0
code:00000011
code:00000013 ; ===== S U B R O U T I N E =====
code:00000013 ; External interrupt 1
code:00000013
code:00000013 ; public IE1
code:00000013 IE1:
code:00000013 mov A, R6
code:00000014 xrl RESERVED0084, A ; RESERVED
code:00000016 mov A, R7
code:00000017 mov A, R6
code:00000018 xrl A, R6
code:00000019 mov A, R6
code:0000001A mov A, R6
code:0000001A ; End of function IE1
code:0000001A
code:0000001B
code:0000001B ; ===== S U B R O U T I N E =====
```


8051 ASSEMBLY?

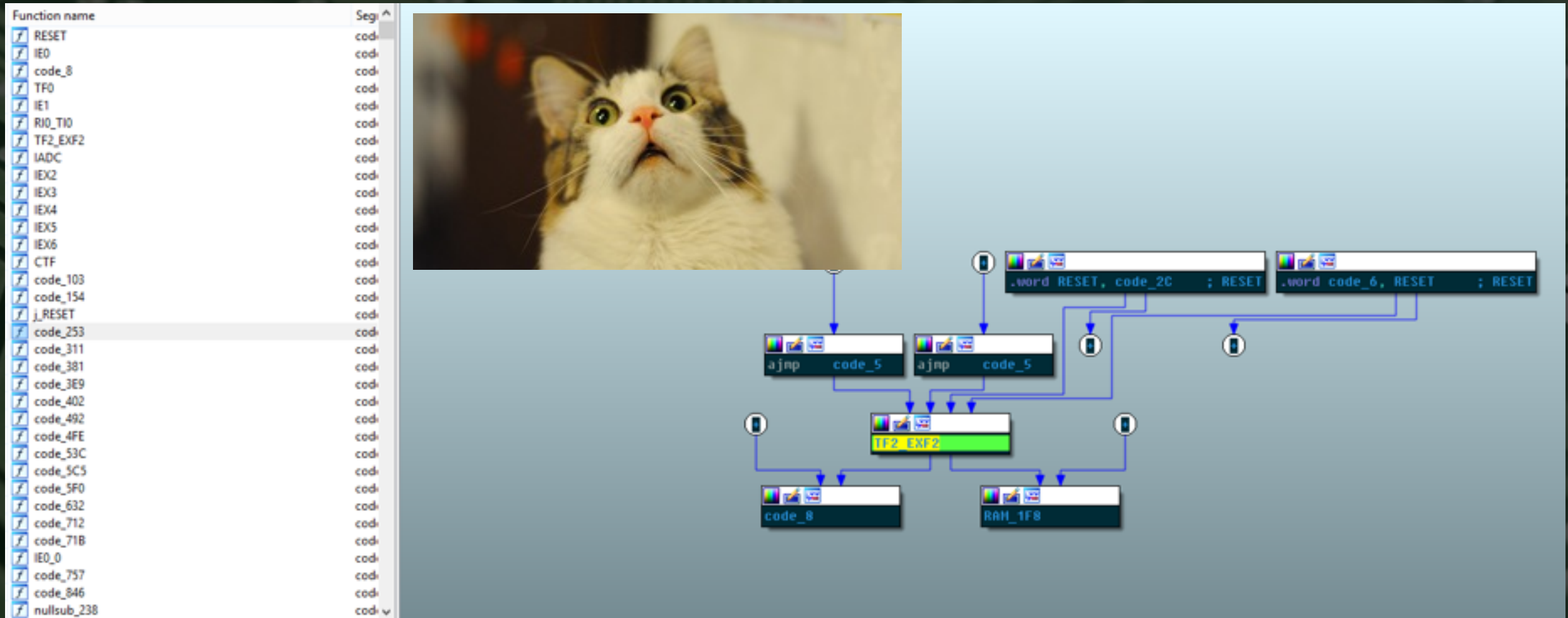
Function name	Seg
IE0	cod
TF0	cod
IE1	cod
TF1	cod
RI0_TI0	cod
IADC	cod
IEX2	cod
IEX5	cod
RI1_TI1	cod
CTF	cod
code_27C	cod
code_27D	cod
code_A03	cod
code_F02	cod
code_1148	cod
code_124F	cod
code_1641	cod
code_183D	cod
code_1BD8	cod
code_2EC3	cod
code_2F3A	cod
code_376D	cod
code_4801	cod
code_488D	cod
code_60D6	cod
code_E9A7	cod
code_EA08	cod
code_EAFF	cod
code_EB03	cod
code_F208	cod
ROM_40100	RON
ROM_402B8	RON
ROM_40608	RON
ROM_40648	RON
ROM_406F8	RON
ROM_4F848	RON
ROM_4FD00	RON
ROM_4FE98	RON
ROM_50044	RON
ROM_50075	RON
ROM_501FB	RON
ROM_50600	RON

```
code:00000000 ; -----  
code:00000000 ; Segment type: Pure code  
code:00000000 ;.segment code  
code:00000000 ; START OF FUNCTION CHUNK FOR CTF  
code:00000000 ; public RESET  
code:00000000 RESET: ; CODE XREF: CTF:code_124↓j  
code:00000000 ; CTF+92↓j ...  
code:00000000 orl A, R5 ; RESET  
code:00000001 anl A, R2  
code:00000001 ; END OF FUNCTION CHUNK FOR CTF  
code:00000001 ; -----  
code:00000002 .byte 0x90 ; É  
code:00000003 ; ----- S U B R O U T I N E -----  
code:00000003 ; External interrupt 0  
code:00000003 ; public IE0  
code:00000003 IE0: nop  
code:00000004 rr A  
code:00000005 nop  
code:00000006 nop  
code:00000007 nop  
code:00000008 inc A  
code:00000009 nop  
code:0000000A nop  
code:0000000A ; End of function IE0  
code:0000000A ; ----- S U B R O U T I N E -----  
code:0000000B ; Timer 0 overflow  
code:0000000B ; public TF0  
code:0000000B TF0: nop  
code:0000000C mov R7, A  
code:0000000D mov R7, A  
code:0000000E nop  
code:0000000F nop  
code:00000010 cjne R0, #0, IE1 ; External interrupt 1  
code:00000010 ; End of function TF0  
code:00000010 ; ----- S U B R O U T I N E -----  
code:00000013 ; -----  
code:00000013 ; -----
```



8051 ASSEMBLY?

EVERYTHING IS 8051!!!

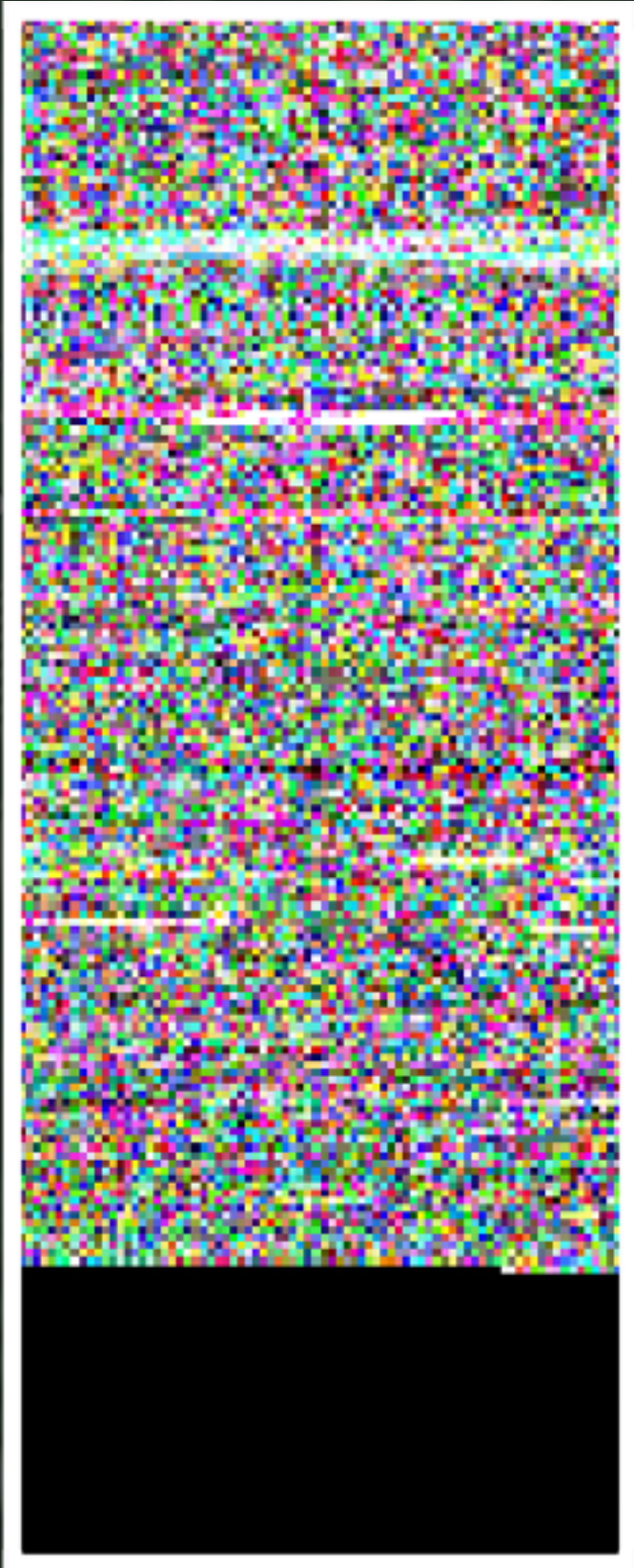


The image shows a screenshot of an IDE interface. On the left, a 'Function name' list includes: RESET, IED, code_8, TF0, IE1, RI0_T10, TF2_EXF2, IADC, IEX2, IEX3, IEX4, IEX5, IEX6, CTF, code_103, code_154, j_RESET, code_253, code_311, code_381, code_3E9, code_402, code_492, code_4FE, code_53C, code_5C5, code_5F0, code_632, code_712, code_71B, IE0_0, code_757, code_846, and nullsub_238. The 'Seg' column shows 'cod' for all entries. In the center, a small image of a surprised-looking cat is displayed. On the right, a flowchart diagram illustrates the execution flow. It starts with two 'RESET' labels at the top, each pointing to a box containing '.word RESET, code_2C ; RESET' and '.word code_6, RESET ; RESET'. Arrows from these boxes lead to two 'ajnp code_5' boxes. These boxes point to a central 'TF2_EXF2' box, which is highlighted in green. From the 'TF2_EXF2' box, arrows point to 'code_8' and 'RAM_1F8' boxes. The background of the IDE is a light blue color.

BREAKING CODE

0000h:	9E 70 61 10 36 10 55 68 60 90 FF 10 4A 58 38 A4	žpa.6.Uh`.y.JX8#
0010h:	47 10 11 10 B5 B0 11 92 E5 11 11 10 DE 8F 11 91	G...μ°. 'á...p...'
0020h:	F8 27 11 10 00 11 11 AF FD AB 7D 90 86 F9 16 1A	ø'.....-ý«}.tù..
0030h:	02 26 22 D0 90 03 AB 07 62 10 83 28 81 A2 87 16	.ε"Đ...«.b.f(.c†.
0040h:	00 EF 42 18 10 62 81 84 1D 07 07 83 10 B0 87 83	.iB..b.....f.°†f
0050h:	83 10 B0 97 07 B8 84 1D 97 90 68 84 B0 07 83 12	f.°-.,...-h...°f.
0060h:	22 08 02 26 07 19 90 87 10 1D D2 07 83 84 B8 07	"..&...†..Ò.f..."
0070h:	07 83 84 B8 E2 83 B8 10 B8 E2 83 68 84 1D 07 90	.f...âf...âfh..."
0080h:	07 22 90 02 26 12 19 10 83 10 B8 26 07 87 84 1D	..&...f.,&.†..."
0090h:	36 07 B8 84 B8 07 83 83 84 B8 07 83 68 10 1D 36	6.,...ff...fh..6
00A0h:	26 07 19 90 02 90 12 22 07 83 84 C0 71 20 87 10	ε....."f...Àq †.
00B0h:	C0 81 83 B8 84 1D 07 07 68 84 1D 07 83 83 10 C0	À.f,...h...ff.À
00C0h:	02 26 12 19 90 81 90 07 97 07 87 84 B0 22 40 83	.&.....-+...°"@f
00D0h:	83 31 07 23 08 20 1D 84 1D 07 07 83 20 B8 E2 23	f1.†.f ,â†
00E0h:	36 07 D0 84 B8 08 83 83 83 70 07 23 08 20 1D 84	6.Đ...fffp.†. ...
00F0h:	1D 07 07 83 20 C0 81 23 27 AF 10 96 42 08 83 F9	...f À.†'-.B.fù
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†.&.Đ...«"ý
0120h:	04 10 45 30 40 75 F9 1E 18 10 E7 01 27 98 C6 70	..EO@uù...ç.'~Ep
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†.&/€.yE8Ò.÷„À@
0160h:	E7 81 1E 98 C6 04 10 07 AF 14 B2 29 F9 29 A3 27	ç...~E...-.°)ù)ε'
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	çS.™E..ò.«Ò+...À.
0190h:	02 26 22 A7 90 03 AB 90 07 AF 90 02 26 22 B6 0A	.f"S...«...-.&"q.
FF00h:	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
FF20h:	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
FF40h:	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
FF60h:	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
FF80h:	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
FFA0h:	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
FFC0h:	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
FFE0h:	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°;i;‰@.'`
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...~~

FIRMWARE DIFFS!

- 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

FIRMWARE DIFFS!

- 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

CAN YOU COUNT?

- 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?

62 75 39 B9 14 16 91 B9 40 B8 B9 B9 D0 67 B8 93	bu9¹..`¹@.¹¹Dg.™
B8 B8 B8 B9 84 9A B8 A0 B8 38 B8 B9 C7 67 B8 B8	...¹„š. .8.¹Çg..
06 B8 8E B9 A9 61 B8 B8 B3 BF 02 39 87 ED D4 50	..Ž¹@a...³ž.9#íÔP
AE 02 B1 79 39 10 8B AA BF 2E B9 81 28 EB 2A 0B	@.±y9.<ªž.¹.(ë*.
2D 28 46 B1 B9 A9 8B EB 2A ED AE 2A B9 B4 AE 01	-(F±¹@<ë*í@*¹´@.
B4 2D B9 FD AE 2A 01 11 68 2A 39 2D 01 FD C1 AE	´-¹ý@*..h*9-.ýÁ@
2E 39 A1 B1 AE 8B 10 CB AE 01 B4 AE 2A B9 3E 2D	.9;±@<.Ë@.´@*¹>-
B9 11 27 01 0E AE 2D 27 39 7E 0E C1 27 01 2A B4	¹.*.®-*®.Á-*
2D B4 98 8A A1 2A AE 89 8A 0E AE 2A 89 B4 AE 01	..š.*@š.®*ž.´@
2A 2A AE 2D 19 5B 79 A1 2D B4 D9 8A A1 2A AE 89	**®-. [y; -´ÛŠ; *®%
8A EF AE 2A 89 B4 AE 19 50 2A 06 3F 8B 8E B9 A1	Ši®*%´@.P*.?<Ž¹;
7F 00 7F 00 FF 11 7F 41 47 43 46 45 44 42 48 49ÿ..AGCFEDBHI
4F 4B 4E 4D 4C 4A 50 51 57 53 56 55 54 52 58 59	OKNMLJPQWSVUTRXY
35 31 34 33 32 5A 36 37 13 39 15 14 30 38 19 20	51432Z67.9..08.
7F 7F 7F 5D 5B 2D 2E 27 01 2C 7E 2F 27 7F 02 03	... [-. ! / ...
64 65 00 6E 00 00 00 65 55 64 00 20 00 00 00 53	..p. ex ...
4B 42 00 20 00 00 00 65 6F 79 00 62 00 00 00 61	de.n...eUd. ...S
38 72 00 64 00 00 03 41 4E 54 00 45 00 00 00 60	KB. ...eoy.b...a
78 20 00 45 00 00 00 74 64 65 00 6E 00 00 00 65	8r.d...ANT.E...`
55 64 00 20 00 00 00 53 4B 42 00 20 00 00 00 65	x .E...tde.n...e
6F 79 00 62 00 00 00 61 06 72 00 64 00 00 03 4B	Ud. ...SKB. ...e
00 00 20 00 69 6D 45 00 00 00 63 00 65 6C 74 00	oy.b...a.r.d...K
00 00 63 00 69 72 38 03 00 00 70 00 70 41 6C 00
00 00 45 00 20 65 78 00 00 00 6E 00 65 74 64 00	..imeE...c.elt.
00 00 20 00 64 65 55 00 00 00 20 00 42 53 4B 00	..c.ir8...p.pAl.
00 00 62 00 79 65 6F 00 00 00 64 00 72 61 05 01	..E. ex...n.etd.
	.. .deU... .BSK.
	..b.yeo...d.ra..

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

ABCDEFGHIJKLMN OPQR STUVWX
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

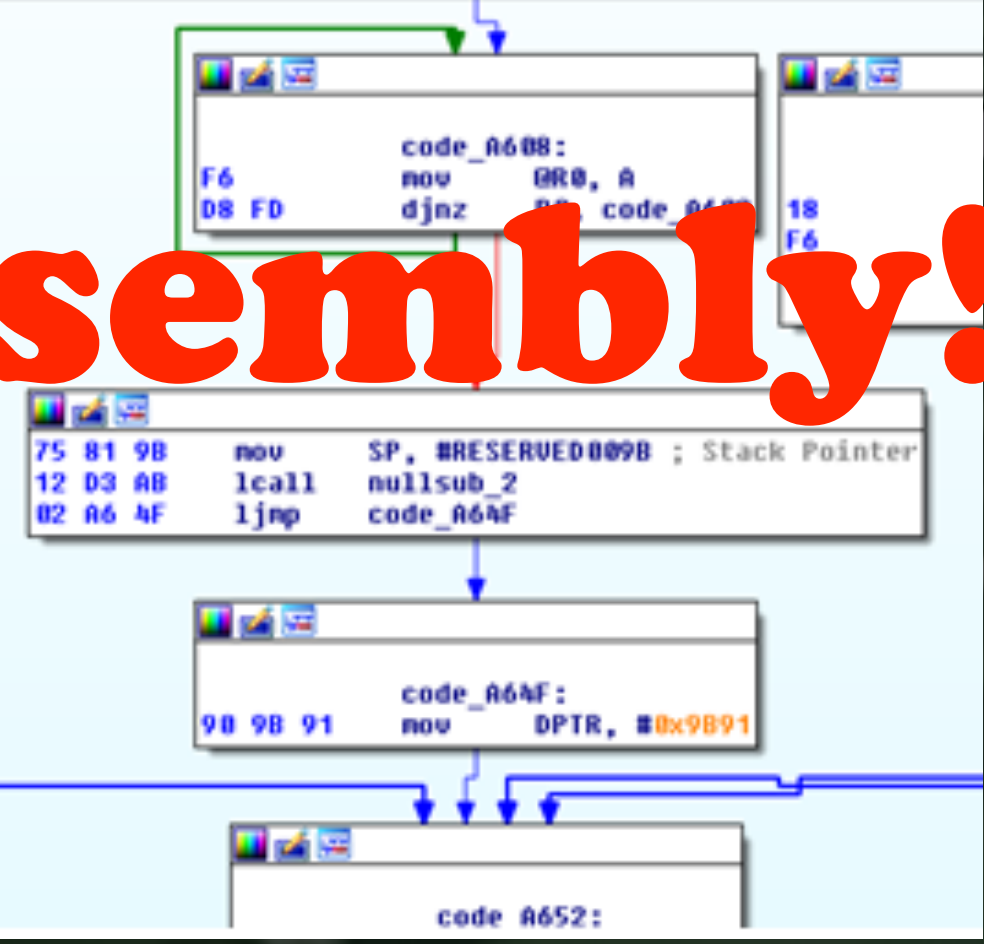
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	34	23	6F	EF	42	40	C7	EF	16	EE	EF	EF	86	31	EE	C5	4#oiB@Çi.iii+liÄ
0010h:	EE	EE	EE	EF	D2	CC	EE	F6	EE	6E	EE	EF	91	31	EE	EE	iiiiÔiioini'lii
0020h:	50	EE	D8	EF	FF	37	EE	EE	E5	E9	54	6F	D1	BB	82	06	Pi0iy7iiaéToN»,.
0030h:	F8	54	E7	2F	6F	46	DD	FC	E9	78	EF	D7	7E	BD	7C	5D	øTç/oFYüéxi~*]
0040h:	7B	7E	10	E7	EF	FF	DD	BD	7C	BB	F8	7C	EF	E2	F8	57	{~.çiyY% »ø iäøW
0050h:	E2	7B	EF	AB	F8	7C	57	47	3E	7C	6F	7B	57	AB	97	F8	â{i«ø WG> o(W«-ø
0060h:	78	6F	F7	E7	F8	DD	46	9D	F8	57	E2	F8	7C	EF	68	7B	xo÷çøYF.øWäø iñ{
0070h:	EF	47	7C	57	58	F8	7B	7C	6F	F8	58	97	7B	57	7C	E2	iG WXø{ øX-(W â
0080h:	EF	9D	DD	46	E7	F8	6F	3E	E2	7B	EF	1D	F8	7C	4F	78	i.YFçø>â{i.ø Ox
0090h:	7C	7C	F8	7B	4F	0D	47	F8	0D	E2	4F	7C	97	7B	F8	EF	ø{O.Gø.âO -(øi
00A0h:	DD	3E	F8	6F	46	E7	9D	6F	EF	78	7C	4F	C9	F8	7B	DF	Y>øøFç.oix OÉø{B
00B0h:	F8	F8	B9	47	7B	4F	7C	E2	4F	EF	7B	F8	7C	97	E2	7C	øø²G{O âO{i ø -â
00C0h:	F8	6F	E7	9D	6F	46	3E	B9	7C	BF	F8	7B	57	AB	78	DD	øøç.oF>² çø(W«xY
00D0h:	7B	E2	CE														{âÛ÷ øBUXø BäøW
00E0h:	7C	7C	F8														ø{O./÷(â.Û÷ øB
00F0h:	DC	B9	F8														Û²ø BäøO. PiYØi÷
0100h:	EF	06	E7														i.çSDýáÐÐ«è,(Oé-
0110h:	FC	78	E5														uxâ>™To..ÝøøFç/T
0120h:	E1	06	EF														á.Iÿçû°Š-9ipØç.g
0130h:	DE	54	DA														PTÛ-Ð.xüPPWÐx^ë»
0140h:	E7	F8	FC														çøüäø..äY-TTäüüi
0150h:	00	6F	78														.oxçÐ.F.çOÇø.°.{
0160h:	F8	EF	7E														øi~g9.âûØ\ëÖ.P)Ö
0170h:	D8	4F	FD														ØOýäøPP^çøÇ.â°,P
0180h:	0D	EF	58														Xf9 çüâOTçüo.{
FF00h:	00	00	00													
FF10h:	00	00	00													
FF20h:	00	00	00													
FF30h:	00	00	00													
FF40h:	00	00	00													
FF50h:	00	00	00													
FF60h:	00	00	00													
FF70h:	00	00	00													
FF80h:	00	00	00													
FF90h:	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	6E	6D	66	76	6E	4D	66	00nmfvnMf.
0000h:																	

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

SUCCESS!!!

```
20E0h: 00 01 22 34 00 07 05 83 03 08 00 05 05 01 09 02  .."4...f.....
20F0h: A1 01 09 01 A1 00 05 09 19 01 29 05 15 00 25 01  ;...i.....)....%.
2100h: 95 05 75 01 81 02 95 01 75 03 81 01 05 01 09 30  *.u...*.u.....0
2110h: 09 31 09 38 15 81 25 7F 75 08 95 03 81 06 C0 C0  .l.8..%.u.*...AA
2120h: 04 03 09 04 22 03 4D 00 69 00 74 00 73 00 75 00  ....".M.i.t.s.u.
2130h: 6D 00 69 00 20 00 45 00 6C 00 65 00 63 00 74 00  m.i. .E.l.e.c.t.
2140h: 72 00 69 00 63 00 38 03 41 00 70 00 70 00 6C 00  r.i.c.s.A.p.p.l.
2150h: 65 00 20 00 45 00 78 00 74 00 65 00 6E 00 64 00  e. .E.x.t.e.n.d.
2160h: 65 00 64 00 20 00 55 00 53 00 42 00 20 00 4B 00  e.d. .U.S.B. .K.
2170h: 65 00 79 00 62 00 6F 00 61 00 72 00 64 00 05 01  e.y.b.o.a.r.d...
2180h: 09 06 A1 01 05 07 19 E0 29 E7 15 00 25 01 75 01  ;...i.....)q...%.u.
2190h: 95 08 81 02 95 01 75 08 81 01 95 05 75 01 05 08  *....u...*.u...
21A0h: 01 29 05 91 02 95 01 03 91 01 95 06 75 08  ;...).'.'.'.*.u.
21B0h: 05 26 00 05 07 19 E0 2A FF 00 81 00 C0 05  ;...49...y...A.
21C0h: 09 08 00 00 00 00 00 00 00 00 00 00 00 00 00  ;...i.....)....%.
21D0h: 00 82 00 09 81 02 95 01 75 03 81 01 05 01 09  ;...u...A
21E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ;...u...u.
21F0h: 08 81 02 95 01 75 03 81 01 05 01 09 30  ;...é...u...è
2200h: 81 02 09 E2 81 06 09 CD 81 06 09 B5 81 06 09 B5  ;...â...i...u...
2210h: 81 22 09 B4 81 22 09 B6 81 06 09 B7 81 06 0A 96  ;...".'.%.g...
2220h: 01 81 06 0A 8A 01 81 06 75 08 81 01 C0 00 00 00  ;.....s...u...â
2230h: 00 00 00 00 00 12 01 10 01 00 00 00 08 57 05 04  ;...
2240h: 20 00 01 01 02 00 01 12 01 10 01 00 00 00 08 57  ;...
2250h: 05 13 22 00 01 01 02 00 01 12 01 10 01 00 00 00  ;...
2260h: 08 57 05 12 22 00 01 01 02 00 01 09 02 3B 00 02  ;...W...".
2270h: 01 00 E0 32 09 04 00 00 01 03 01 01 04 09 21 00  ;...&2.....!..
2280h: 01 00 01 22 41 00 07 05 81 03 08 00 0A 09 04 01  ;...".A.....
2290h: 00 01 03 01 02 00 09 21 00 01 00 01 22 34 00 07  ;...!...."4..
22A0h: 05 83 03 08 00 05 09 02 3B 00 02 01 00 E0 32 09  ;...f.....?....&2.
22B0h: 04 00 00 01 03 01 01 04 09 21 00 01 00 01 22 41  ;...!...."A
22C0h: 00 07 05 81 03 08 00 0A 09 04 01 00 01 03 01 02  ;...
22D0h: 00 09 21 00 01 00 01 22 56 00 07 05 83 03 08 00  ;...!...."V...f...
22E0h: 05 04 03 09 04 0A 03 41 00 54 00  ;...
22F0h:  ;...
2300h: 00 20 00 56 00 34 00 2E 00 31 00 2E 00 34 00 30  ;... .V.4...1...4.0
2310h: 00 31 00 24 03 43 00 53 00  ;... .l.s.c.
2320h: 00 20 00 56 00 34 00 2E 00 31 00 2E  ;... .V.4...1..
2330h: 00 34 00 30 00 31 00 06 03 4B 00 62 00 06 03 4D  ;... .4.0.1...K.b...M
2340h: 00 73 00 05 01 09 06 A1 01 05 07 19 E0 29 E7 15  ;... .a.....;...i.....)q...%.u.
2350h: 00 25 01 75 01 95 08 81 02 95 01 75 08 81 01 95  ;... .%.u...*.u...*
```

```
RESET_0:
; FUNCTION CHUNK AT 00009DDF SIZE 000000AB BYTES
; FUNCTION CHUNK AT 0000A002 SIZE 00000003 BYTES
75 F6 87  nov    CHPENR, #0x87 ; 'ç' ; RESERVED
75 F6 59  nov    CHPENR, #0x59 ; 'Y' ; RESERVED
74 EF     nov    A, #0xEF ; 'n'
52 BF     anl    RESERVED000F, A ; RESERVED
75 F6 00  nov    CHPENR, #0 ; RESERVED
78 FF     nov    R0, #0xFF
E4        clr    A
```



Strings! 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.



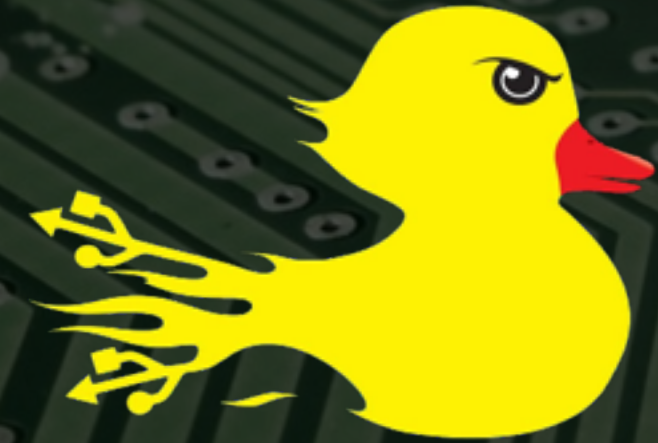
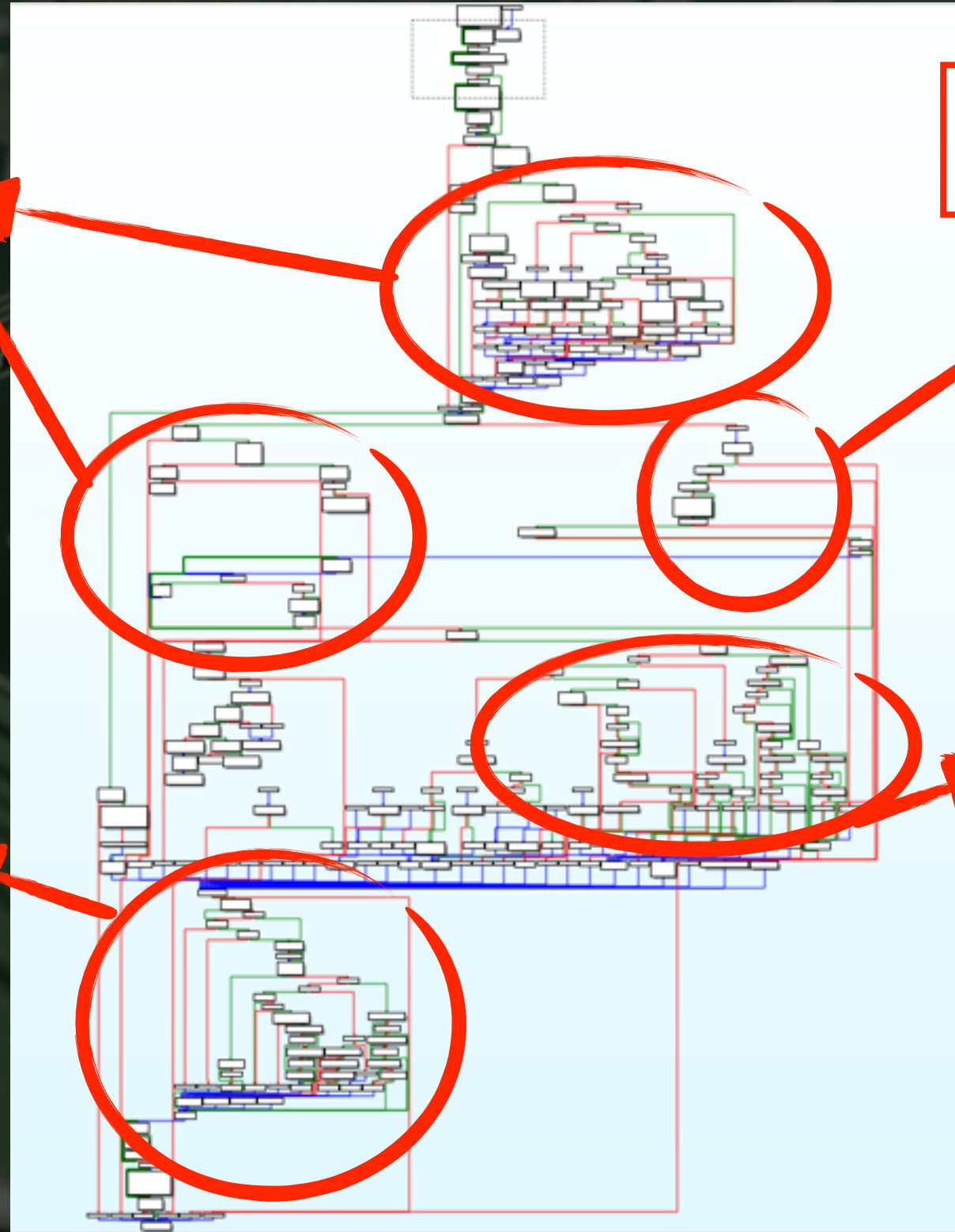
KVMLOGIC

Keyboard
Emulation

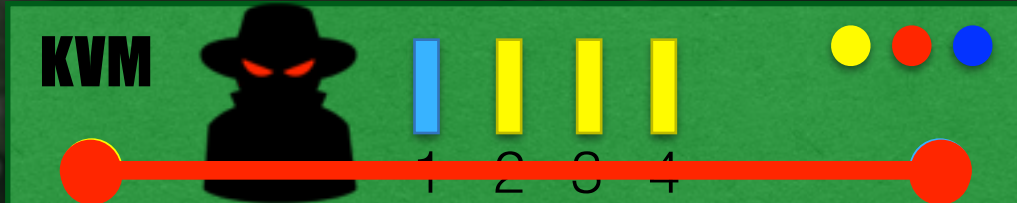
HID Parsing

Hotkeys
Handling

Keyboard
LEDs
Control



“HELLO KVM!”



**Air Gapped
Network**

**Internet Connected
Network**



The background is a dark green, almost black, surface with a complex, glowing circuit board pattern. The pattern consists of numerous thin, light green lines that form a dense, interconnected network of paths and nodes. The lines vary in thickness and are arranged in a way that suggests a complex electronic layout. The overall effect is a sense of depth and technical precision.

DEMO**TIME**

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

