# 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

Lior Oppenheim

“The mad scientist”

Security Researcher

Check Point Software Technologies

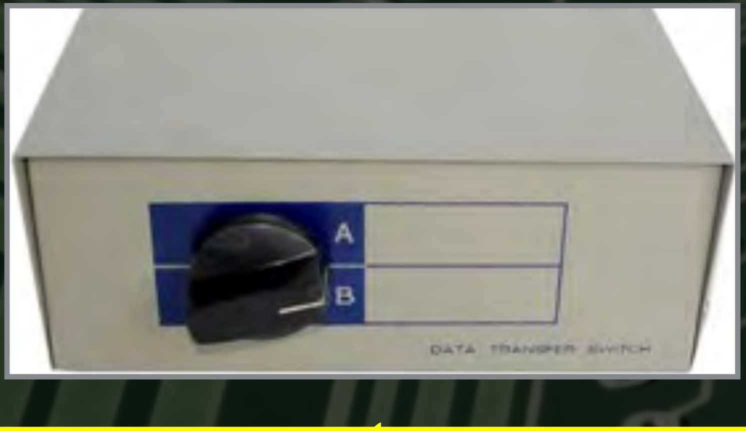
# TOOMANYCOMPUTERS

- Computers
- More 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.

# KVMEVOLUTION



1981

`A-B Switch`

2002

Desktop KVM

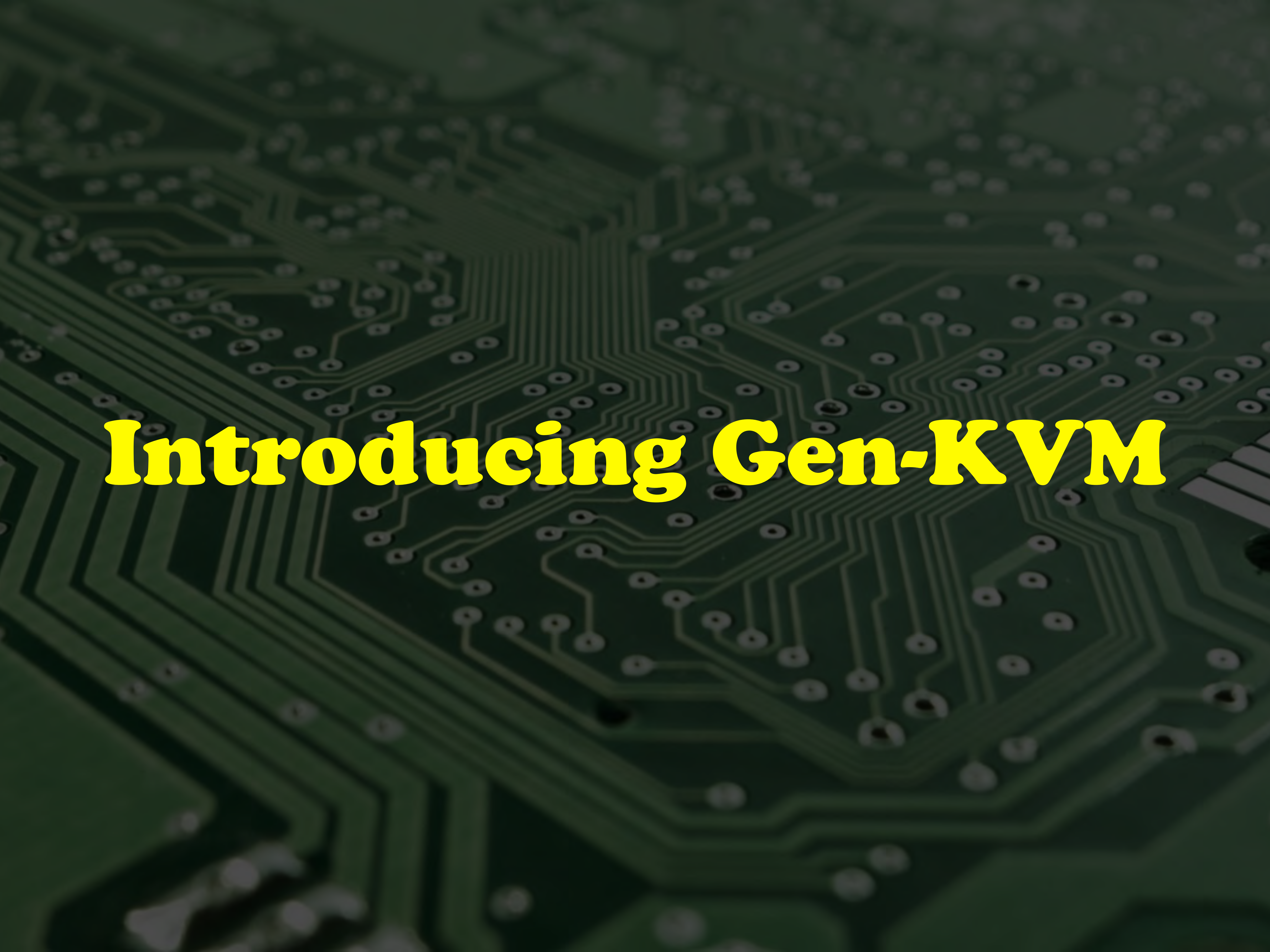
2015

Enterprise KVM

# WHEREARETHEY?

- On top of your server racks.
- On your desktop.
- In your security centres.

**KVMS ARE EVERYWHERE!!**



# Introducing Gen-KVM

# ITRUNSCODE

- On screen configuration display.

+

- Configurable hot-keys.

+

- Control device functionality through keyboard.

=

**Exploitable?**

# First Attempt

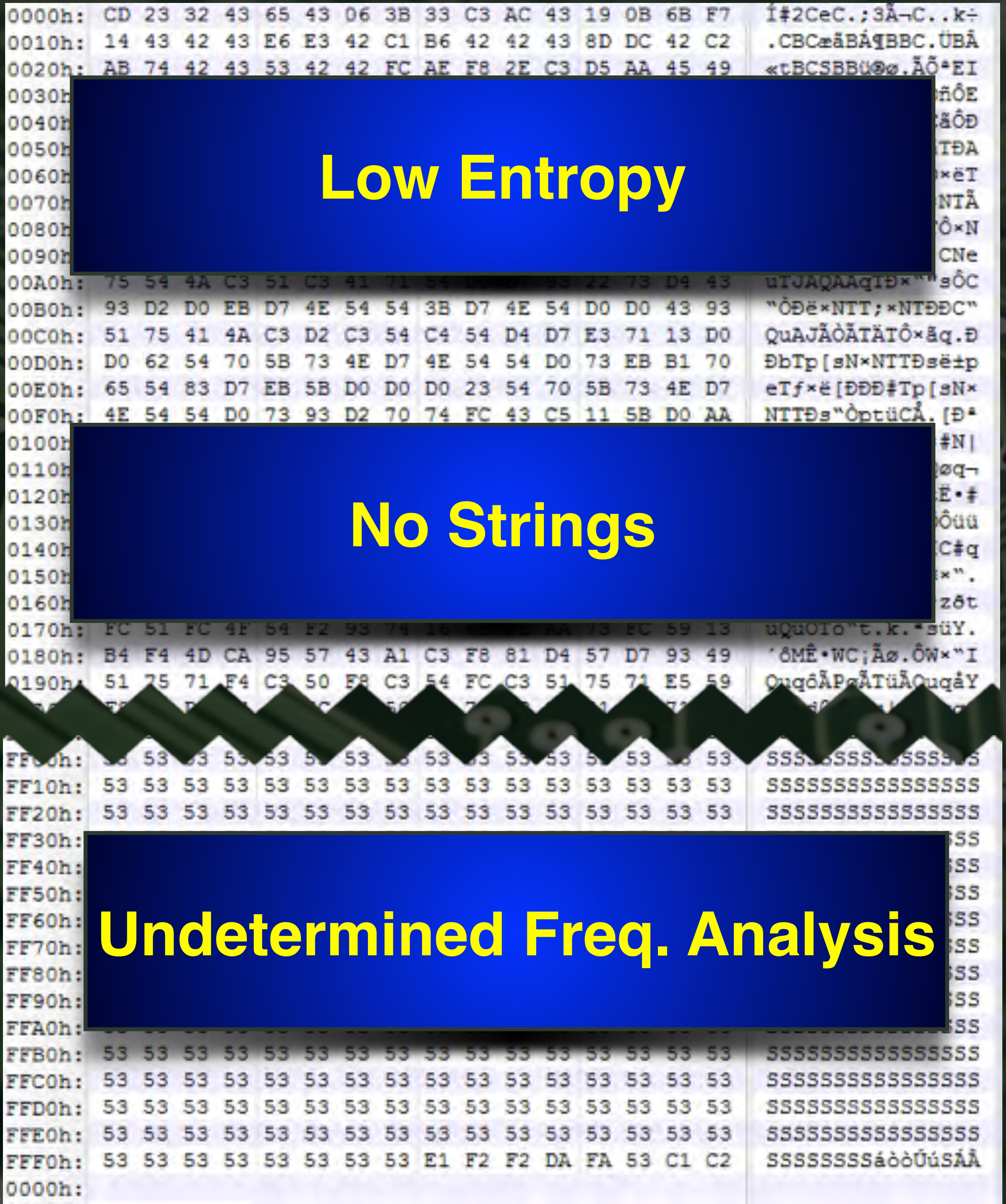
(Funny meme here)

# SOFTWARE

CHALLENGE ACCEPTED!!

- Opening the KVM box.
- Manuals, Cables, Warranty and CD…
- CD contains **A Firmware Upgrade Utility!**
- Can the firmware be extracted from the upgrade utility?!
- Since x86 is no new territory. we can reverse engineer this!

# MEETTHEBLOB



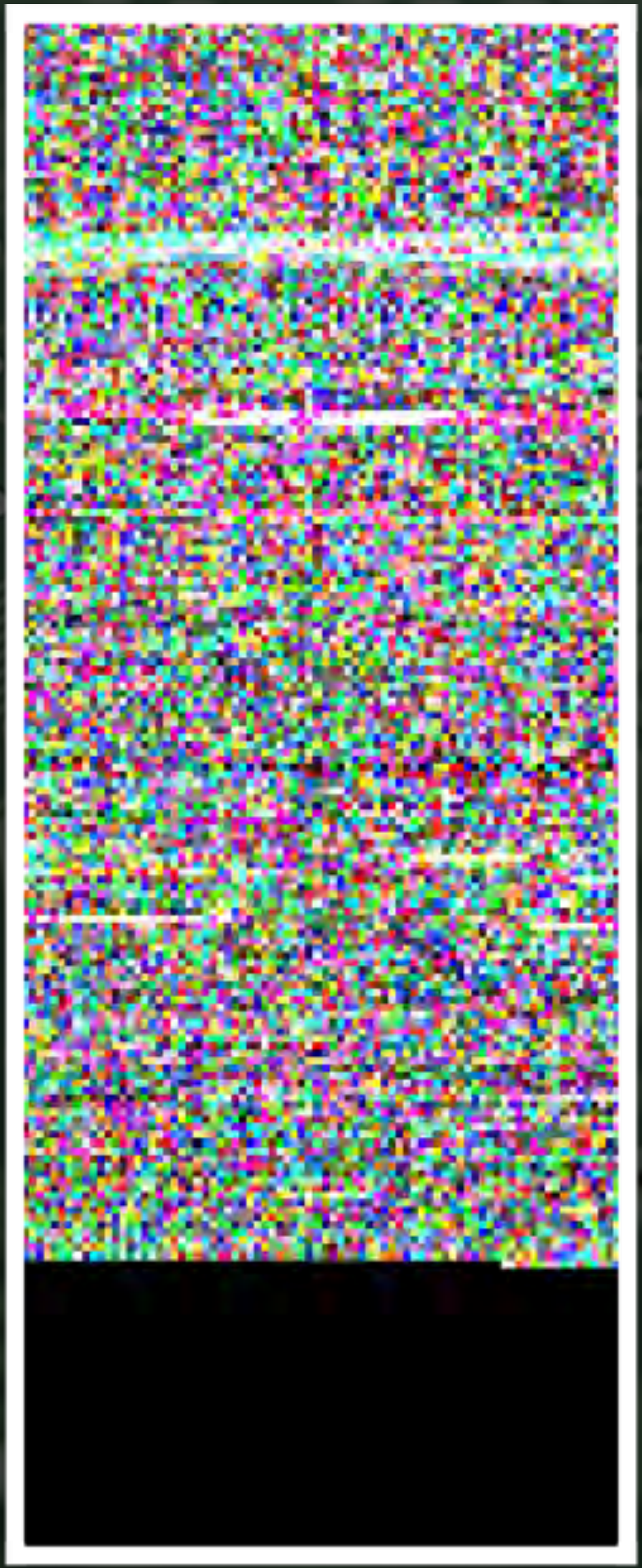
```
0000h: CD 23 32 43 65 43 06 3B 33 C3 AC 43 19 0B 6B F7   Í#2CeC.;3Ã¬C..k÷
0010h: 14 43 42 43 E6 E3 42 C1 B6 42 42 43 8D DC 42 C2   .CBCæãBÁ¶BBC.ÜBÂ
0020h: AB 74 42 43 53 42 42 FC AE F8 2E C3 D5 AA 45 49   «tBCSBBü®ø.ÃÕªEI
0030h                                                       ñÔE
0040h                                                       ãÔÐ
0050h                                                       TÐA
0060h                                                       ×ëT
0070h                                                       NTÃ
0080h                                                       Ô×N
0090h                                                       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                                                       #N|
0110h                                                       øq¬
0120h                                                       Ë•‡
0130h                                                       Ôüü
0140h                                                       C#q
0150h                                                       ×".
0160h                                                       zôt
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:                                                      SS
FF40h:                                                      SS
FF50h:                                                      SS
FF60h:                                                      SS
FF70h:                                                      SS
FF80h:                                                      SS
FF90h:                                                      SS
FFA0h:                                                      SS
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   SSSSSSSSáòòÚúSÁÂ
0000h:
```

**Low Entropy**

**No Strings**

**Undetermined Freq. Analysis**



# FAIL!

# SERIALSNIFF

CHALLENGE ACCEPTED!!

- Firmware upgrade process is done via a custom serial connection.
- It is possible to extract the (possibly) decoded firmware binary from the serial protocol.
- Its 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
```

Data Transfer

```
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.=*

                        • • •

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 Device

🟨 To Device

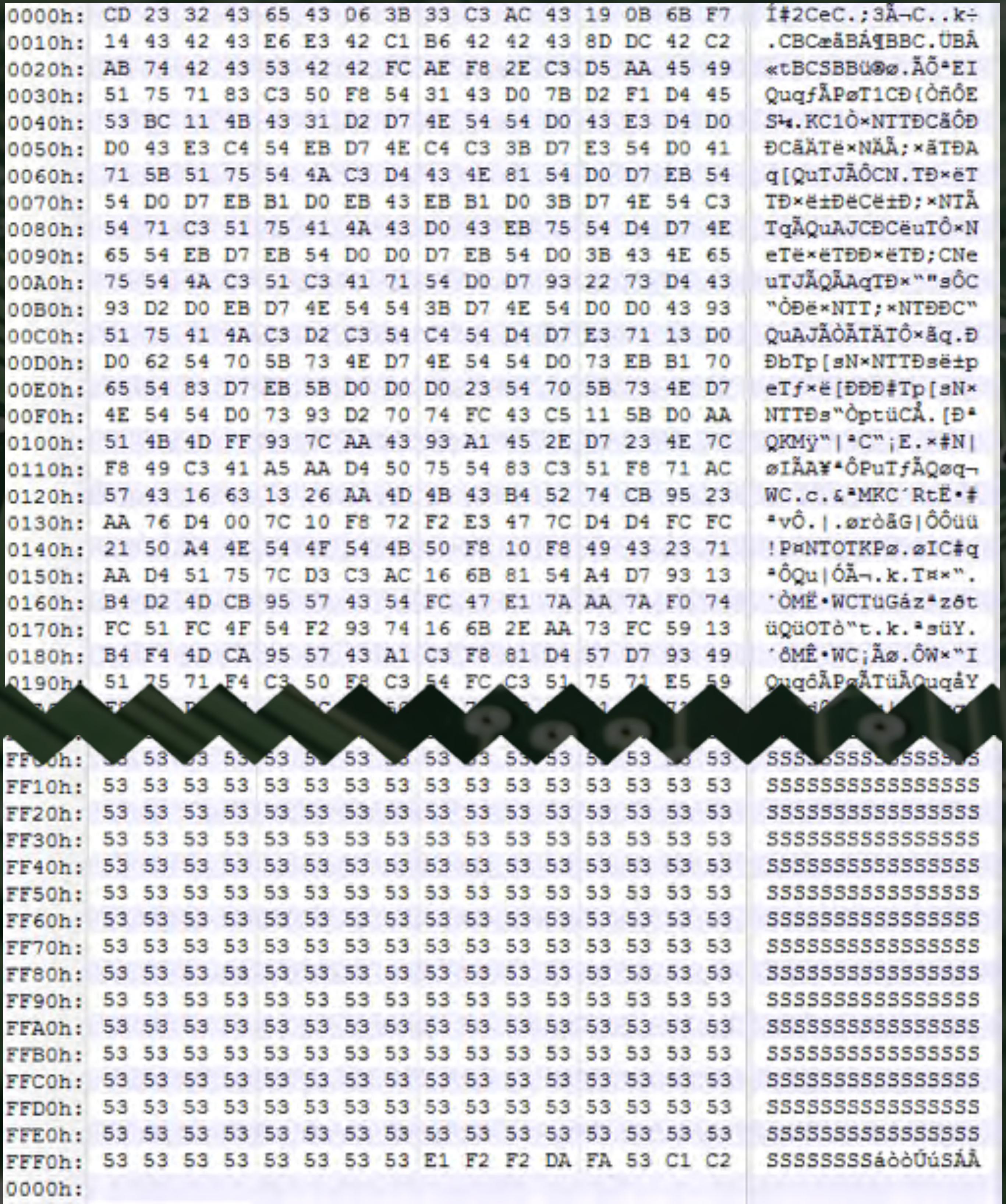
🟦 Fixed Header

⬜ OpCode

🟦 Seq. Number

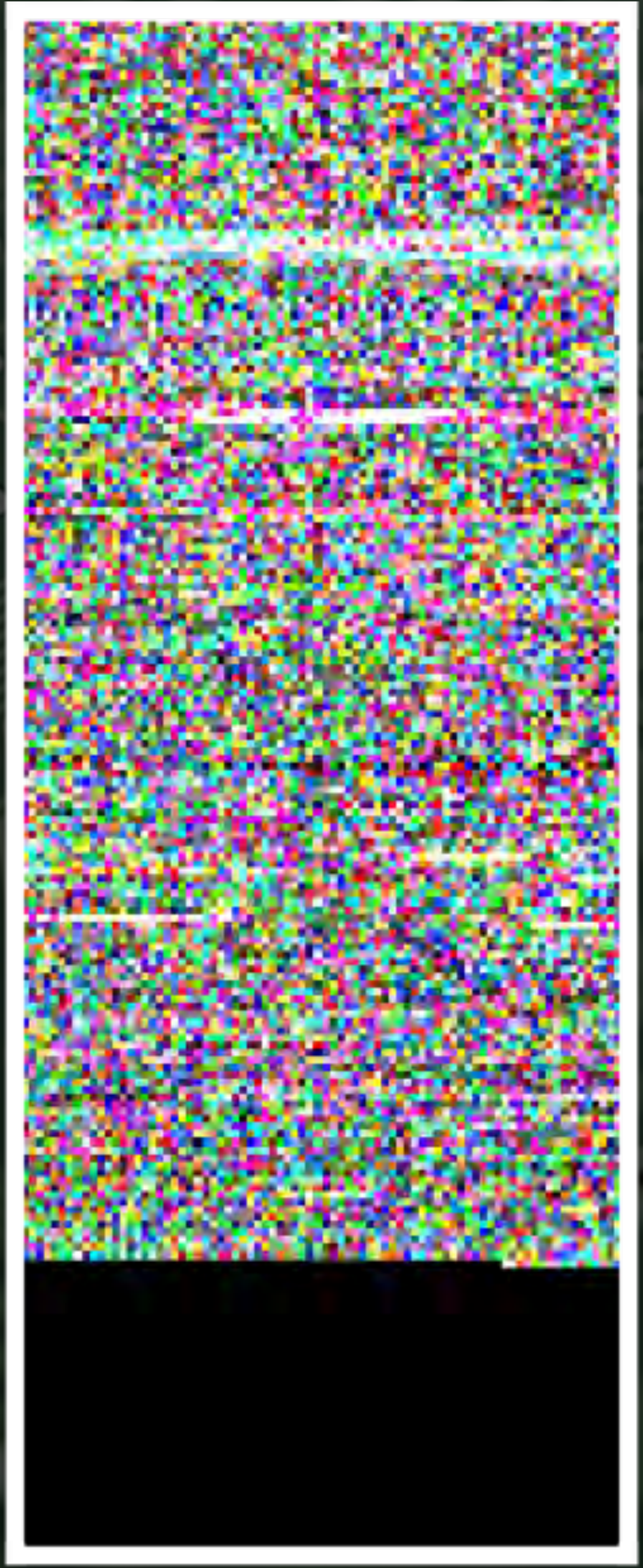
🟧 CheckSum

# GUESSWHO?



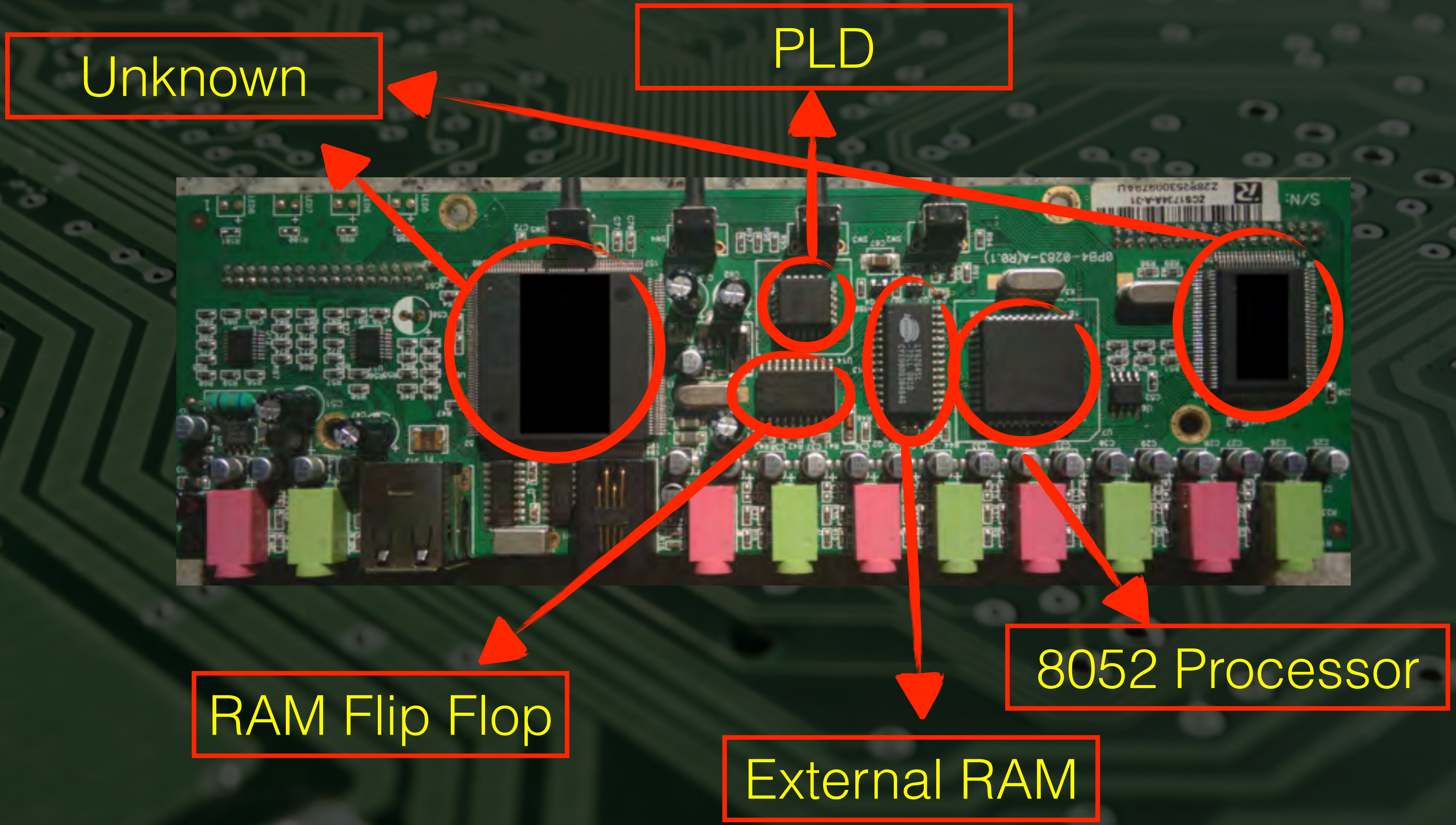
```
0000h: CD 23 32 43 65 43 06 3B 33 C3 AC 43 19 0B 6B F7  Í#2CeC.;3Ã¬C..k÷
0010h: 14 43 42 43 E6 E3 42 C1 B6 42 42 43 8D DC 42 C2  .CBCæãBÁ¶BBC.ÜBÂ
0020h: AB 74 42 43 53 42 42 FC AE F8 2E C3 D5 AA 45 49  «tBCSBBü®ø.ÃÕªEI
0030h: 51 75 71 83 C3 50 F8 54 31 43 D0 7B D2 F1 D4 45  QuqƒÃPøT1CÐ{ÒñÔE
0040h: 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¡ÃøÔW×"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  SSSSSSSSáòòÚúSÁÂ
0000h:
```



# FAIL!

# PCBLAYOUT



Unknown

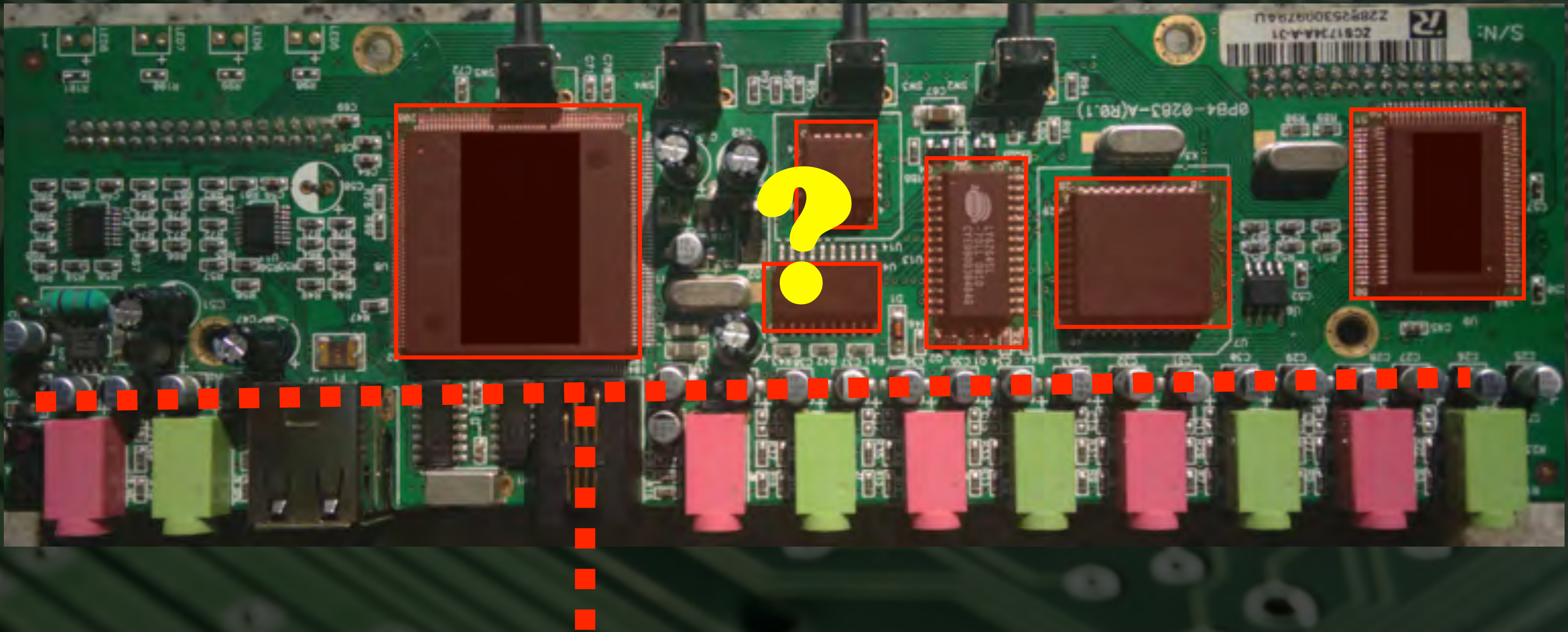
PLD

RAM Flip Flop

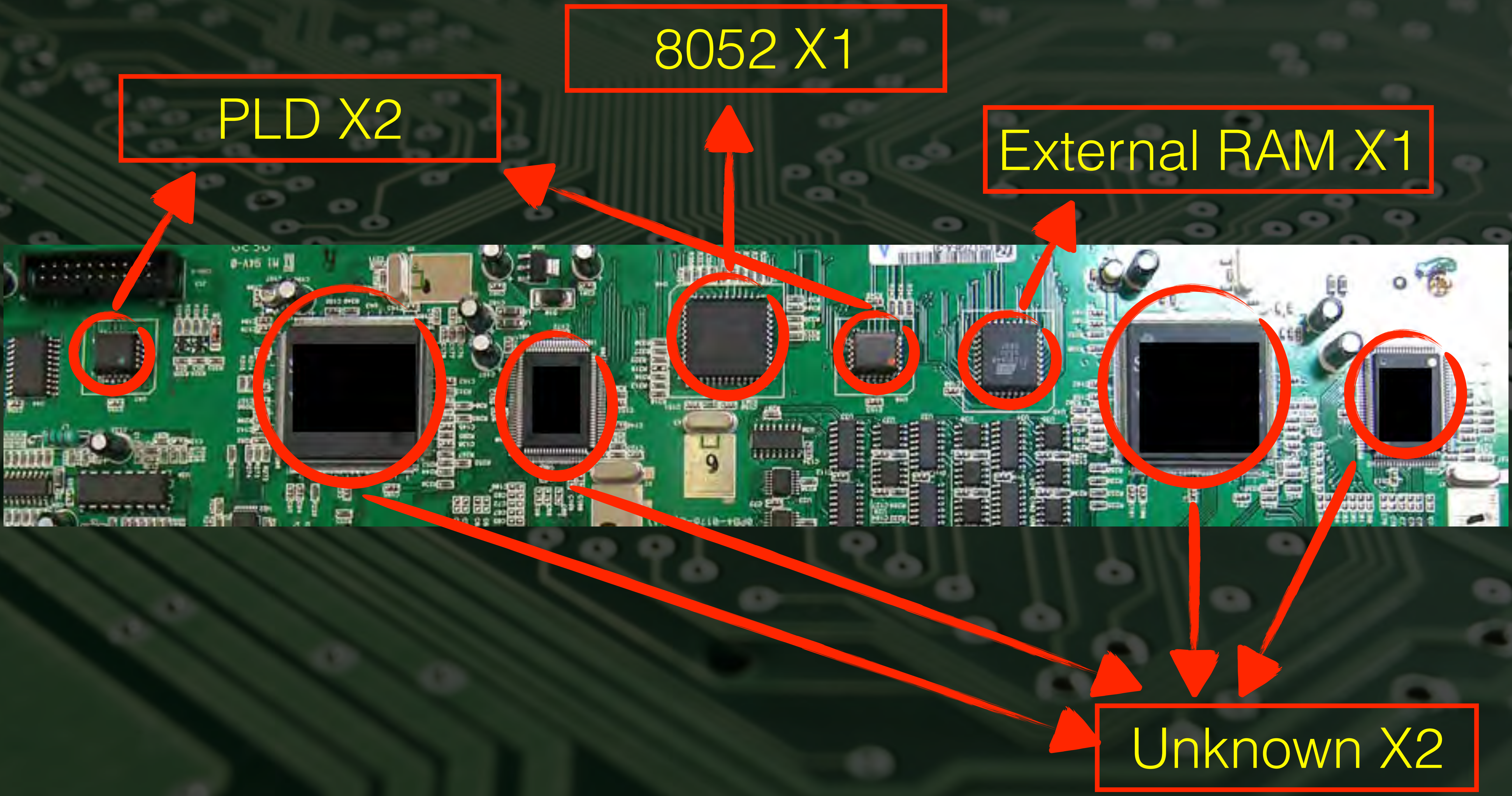
External RAM

8052 Processor

# PCBLAYOUT



# PCBLAYOUT



8052 X1

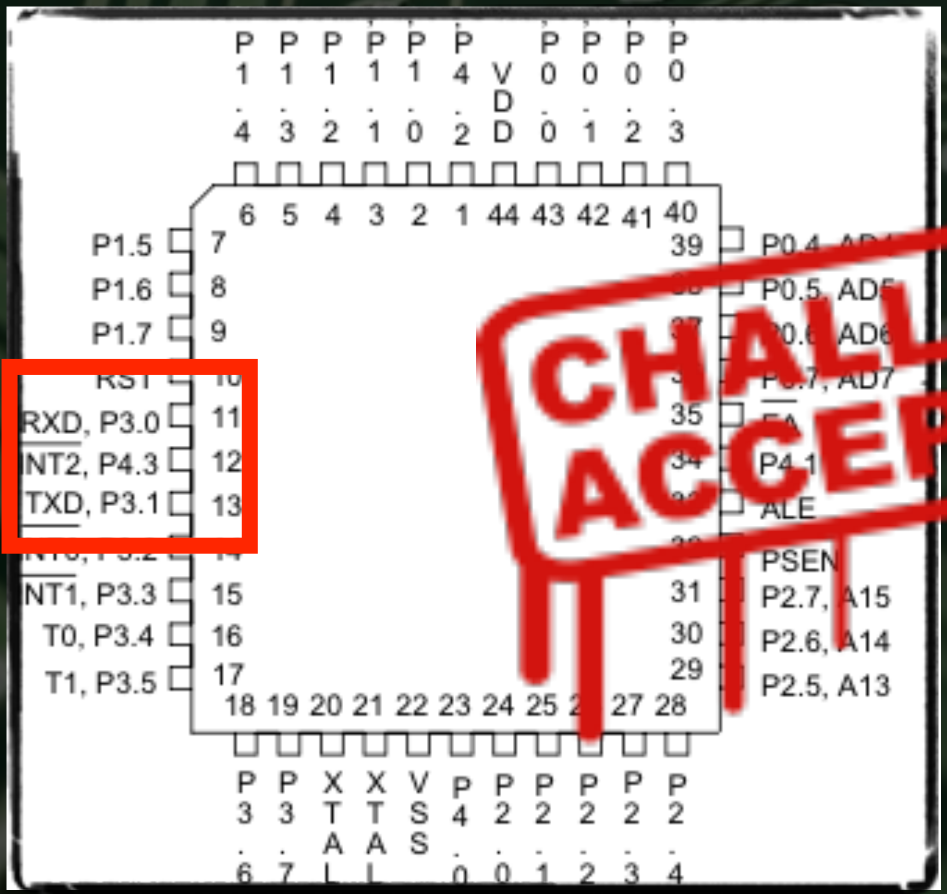
PLD X2

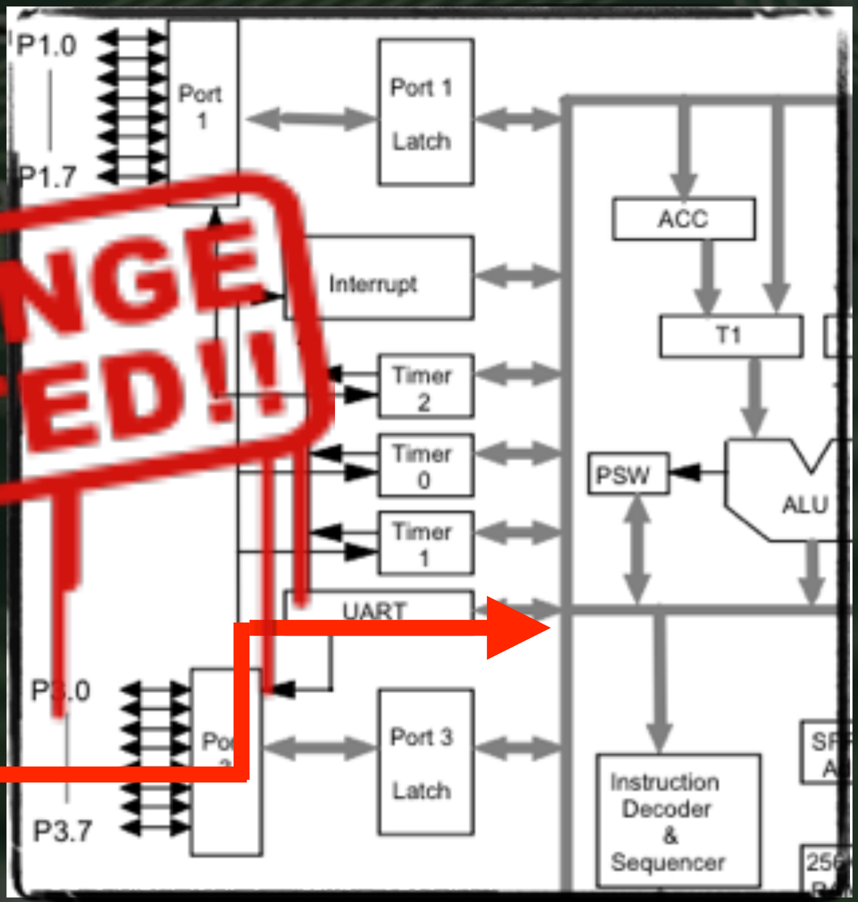
External RAM X1

Unknown X2

# UARTMAGIC

- 8051\2 Chips have an integrated UART port.
- Which IC pins should be tapped?
- If we find out, the firmware could be extracted using simple LOGIC.



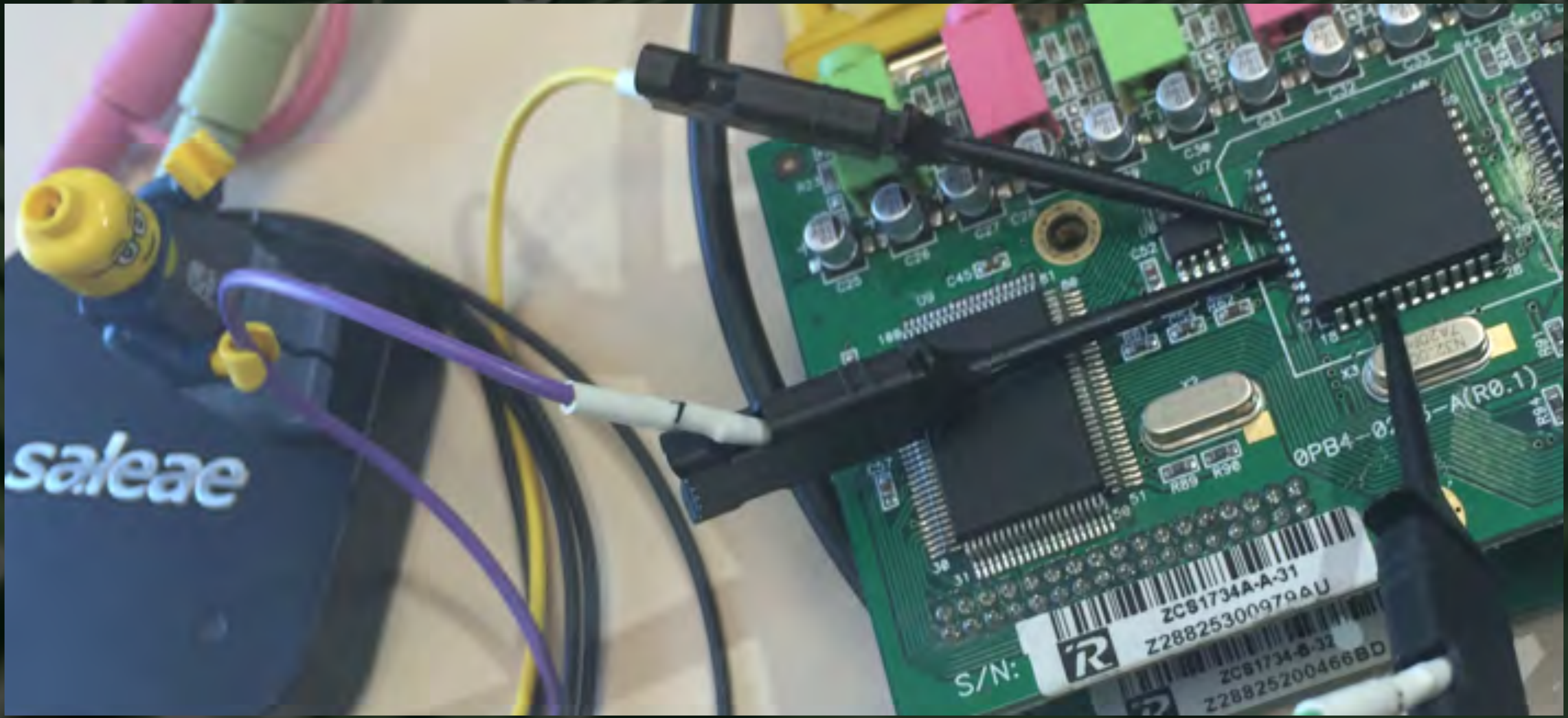


# NOTHINGBUTLOGIC

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

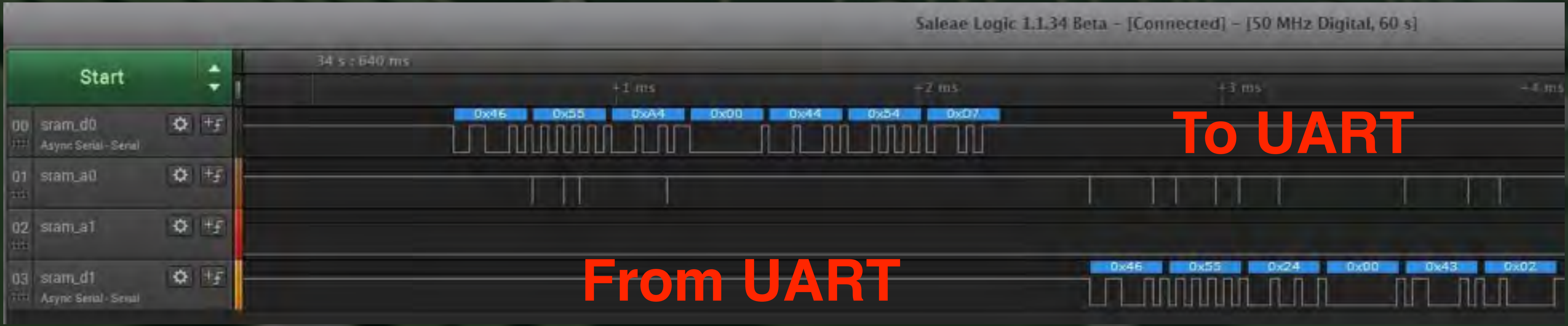
# TAPICPINS

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



# SIGNALANALYSIS

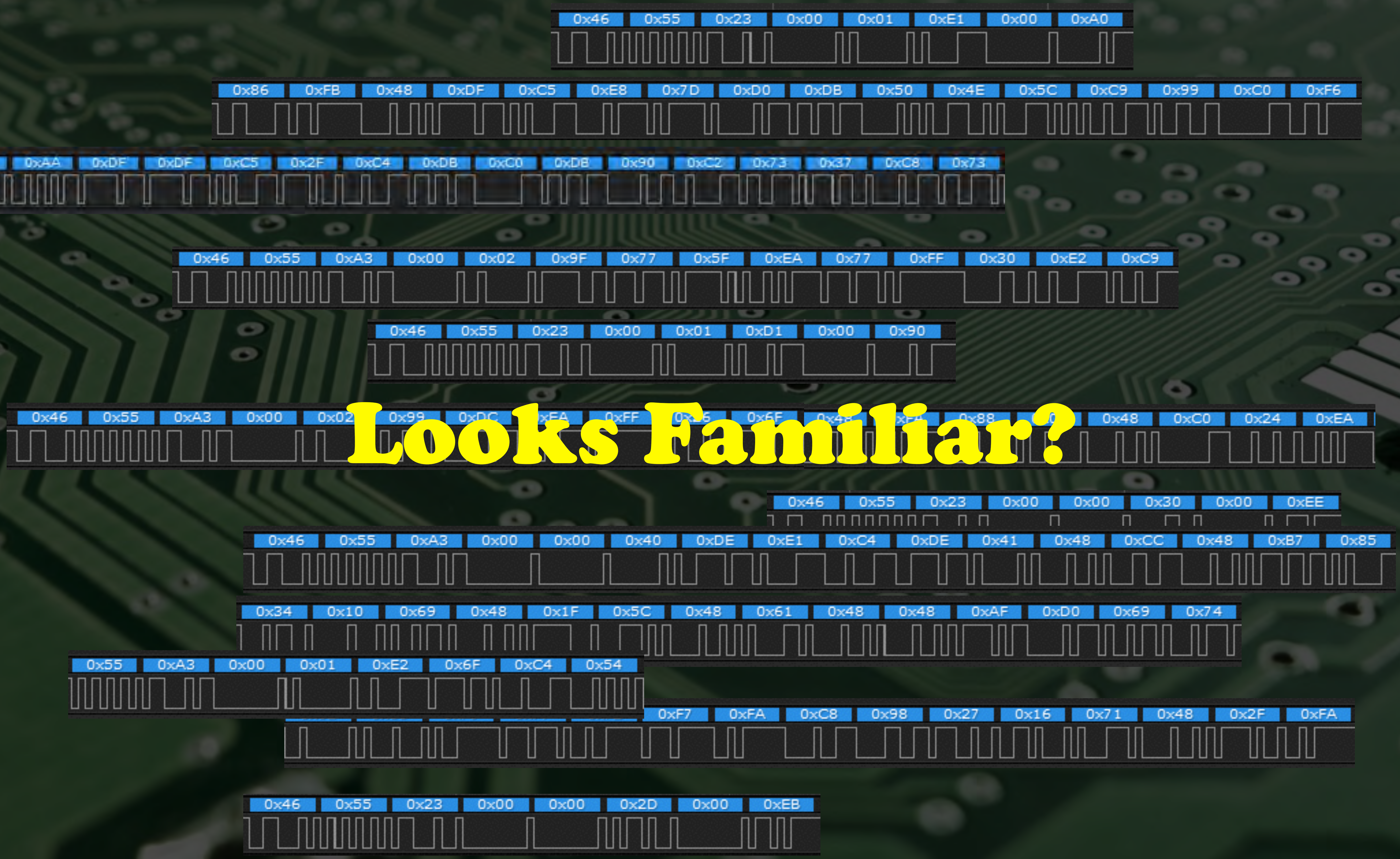
- Reviewing the signals in the UI.
- An obvious pattern emerges.



To UART

From UART

# GREATSUCCESS?



```
0x46 0x55 0x23 0x00 0x01 0xE1 0x00 0xA0
0x86 0xFB 0x48 0xDF 0xC5 0xE8 0x7D 0xD0 0xDB 0x50 0x4E 0x5C 0xC9 0x99 0xC0 0xF6
0xAA 0xDF 0xDF 0xC5 0x2F 0xC4 0xDB 0xC0 0xDB 0x90 0xC2 0x73 0x37 0xC8 0x73
0x46 0x55 0xA3 0x00 0x02 0x9F 0x77 0x5F 0xEA 0x77 0xFF 0x30 0xE2 0xC9
0x46 0x55 0x23 0x00 0x01 0xD1 0x00 0x90
0x46 0x55 0xA3 0x00 0x02 0x99 0xDC 0xEA 0xFF [illegible] 0x6F 0x48 [illegible] 0x88 [illegible] 0x48 0xC0 0x24 0xEA
0x46 0x55 0x23 0x00 0x00 0x30 0x00 0xEE
0x46 0x55 0xA3 0x00 0x00 0x40 0xDE 0xE1 0xC4 0xDE 0x41 0x48 0xCC 0x48 0xB7 0x85
0x34 0x10 0x69 0x48 0x1F 0x5C 0x48 0x61 0x48 0x48 0xAF 0xD0 0x69 0x74
0x55 0xA3 0x00 0x01 0xE2 0x6F 0xC4 0x54
0xF7 0xFA 0xC8 0x98 0x27 0x16 0x71 0x48 0x2F 0xFA
0x46 0x55 0x23 0x00 0x00 0x2D 0x00 0xEB
```

## Looks Familiar?

# 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     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.=*
```

• • •

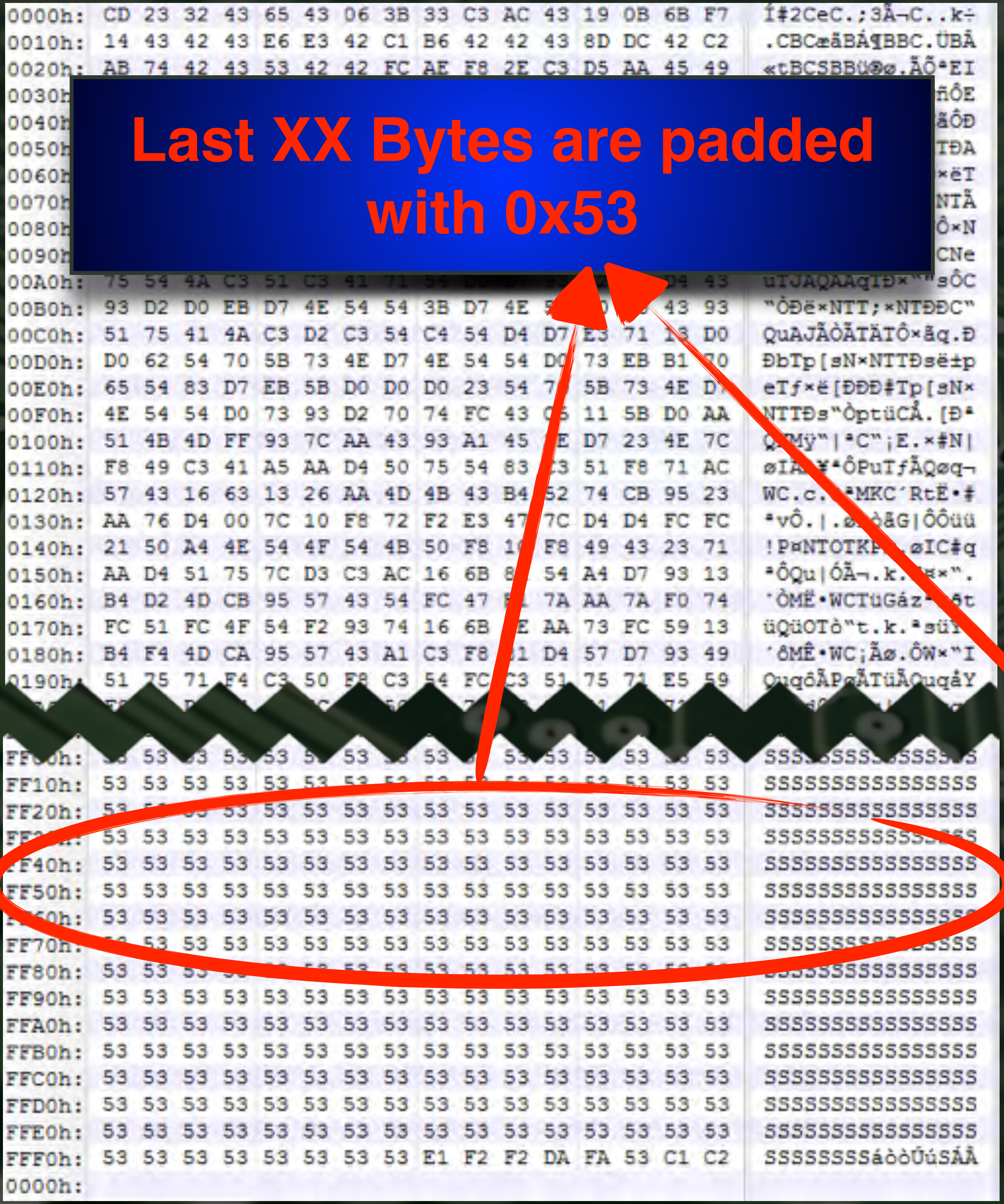
```
46 55 a3 00 03 63 40 d7 85 85 32 ea e2 01 6b 85    FU£..c@◊ÖÖ2Í,.kÖ
32 a6 d9 d6 e5 df 55 a6 d5 22 04 d6 cd 05 d5 96    2¶Ÿ÷ÂﬂU¶’".÷Õ.’ñ
27 85 85 d7 40 a5 d7 32 01 32 e2 85 6b ea 85 d9    'ÖÖ◊@•◊2.2,ÖkÍÖŸ
df d5 e5 a6 55 d6 a6 04 2d 27 cd 22 d5 d6 96 85    ﬂ’Â¶U÷¶.-'Õ"’÷ñÖ
a5 01 40 85 d7 d7 81    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

# BREAKINGCODE

CHALLENGE ACCEPTED!!

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

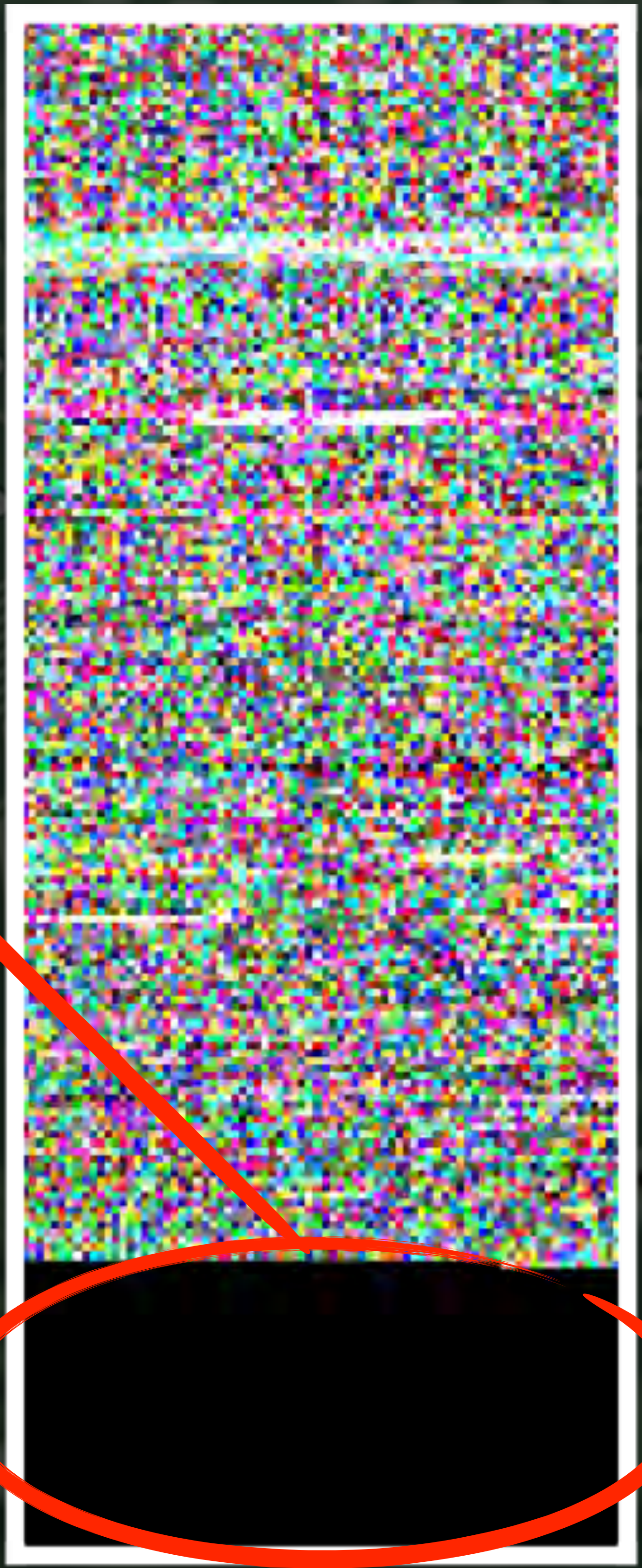
# REMEETTHEBLOB



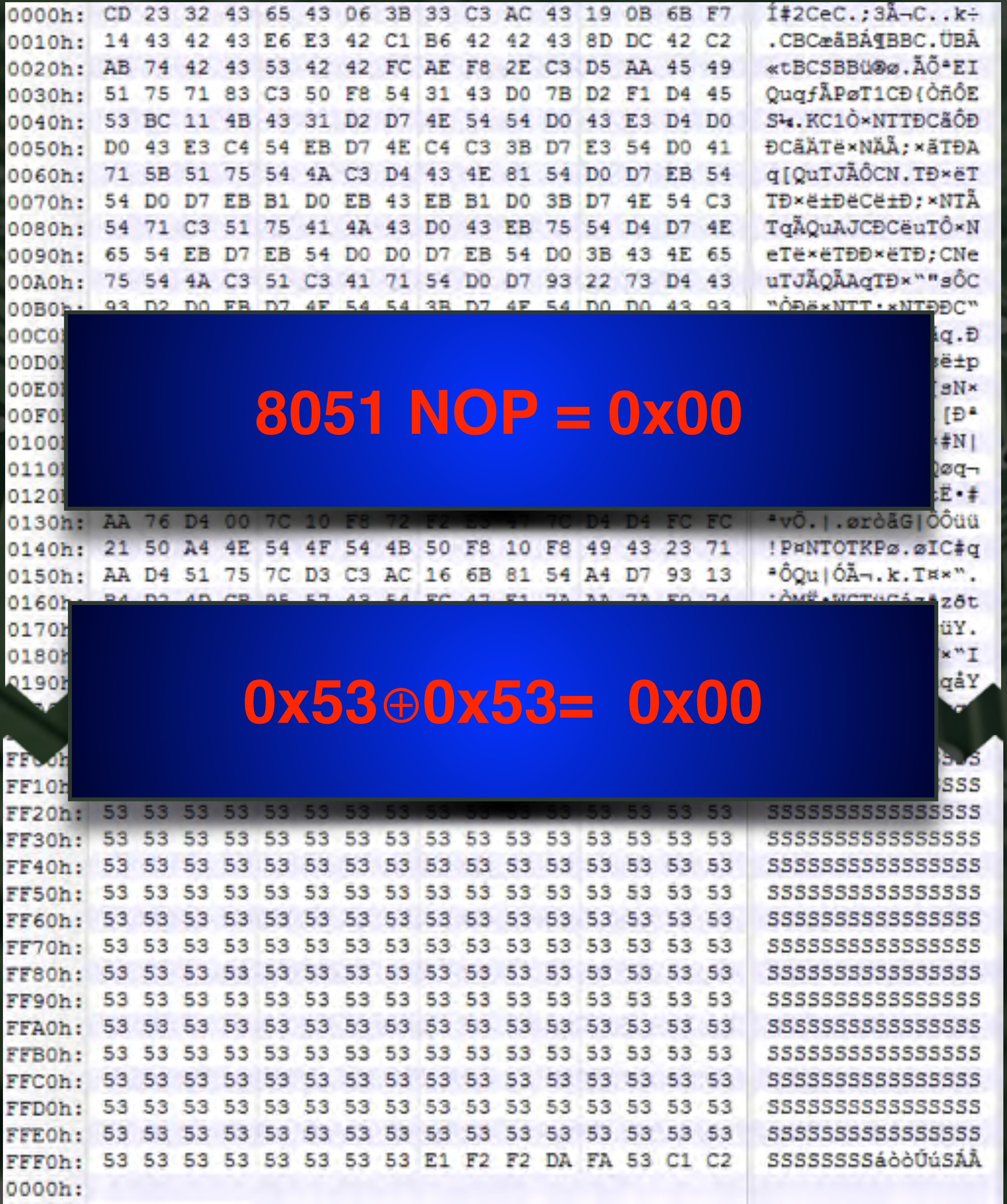
```
0000h: CD 23 32 43 65 43 06 3B 33 C3 AC 43 19 0B 6B F7  Í#2CeC.;3Ã¬C..k÷
0010h: 14 43 42 43 E6 E3 42 C1 B6 42 42 43 8D DC 42 C2  .CBCæãBÁ¶BBC.ÜBÂ
0020h: AB 74 42 43 53 42 42 FC AE F8 2E C3 D5 AA 45 49  «tBCSBBü®ø.ÃÕªEI
0030h                                                   ñÔE
0040h                                                   ãÔÐ
0050h                                                   TÐA
0060h                                                   ×ëT
0070h                                                   NTÃ
0080h                                                   Ô×N
0090h                                                   CNe
00A0h: 75 54 4A C3 51 C3 41 71 54 D0 D7 93 94 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 1E 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 8E 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  SSSSSSSSáòòÚúSÁÂ
0000h:
```

Last XX Bytes are padded with 0x53



# BREAKINGCODE



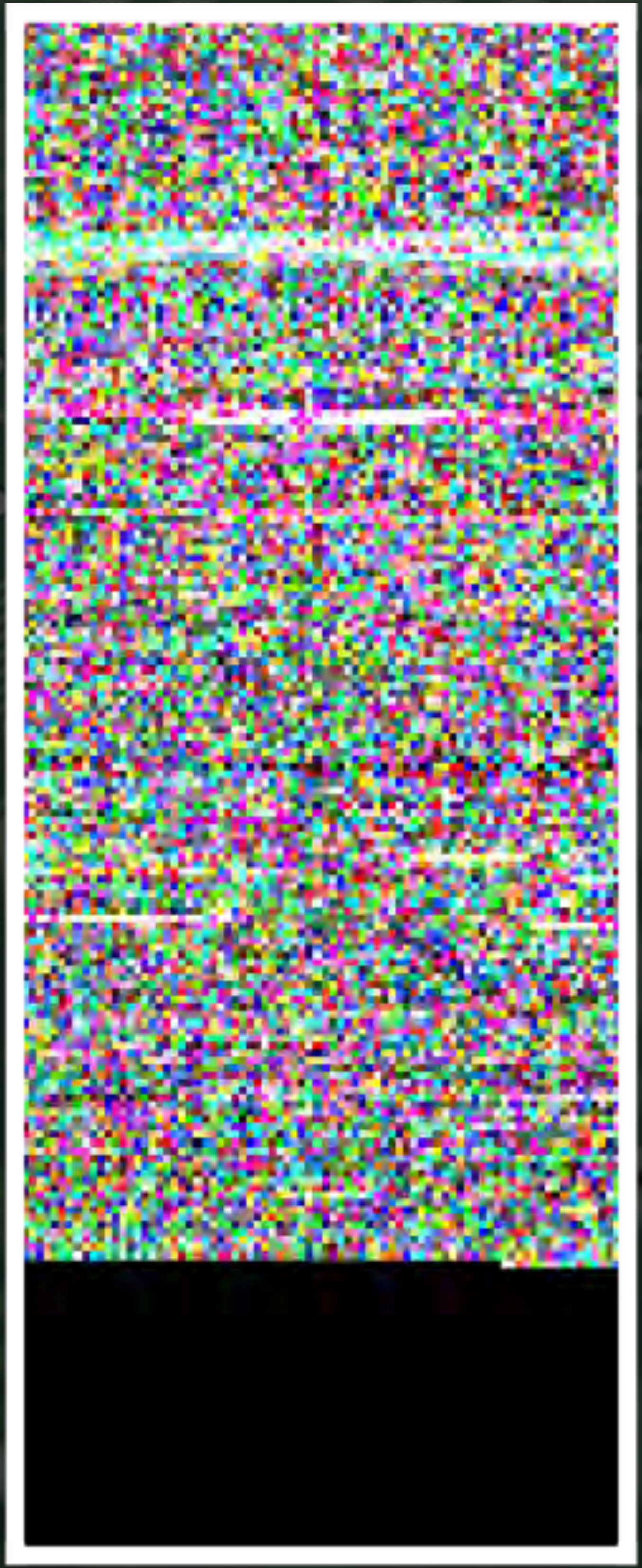
```
0000h: CD 23 32 43 65 43 06 3B 33 C3 AC 43 19 0B 6B F7  Í#2CeC.;3Ã¬C..k÷
0010h: 14 43 42 43 E6 E3 42 C1 B6 42 42 43 8D DC 42 C2  .CBCæãBÁ¶BBC.ÜBÂ
0020h: AB 74 42 43 53 42 42 FC AE F8 2E C3 D5 AA 45 49  «tBCSBBü®ø.ÃÕªEI
0030h: 51 75 71 83 C3 50 F8 54 31 43 D0 7B D2 F1 D4 45  QuqƒÃPøT1CÐ{ÒñÔE
0040h: 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“
```

8051 NOP = 0x00

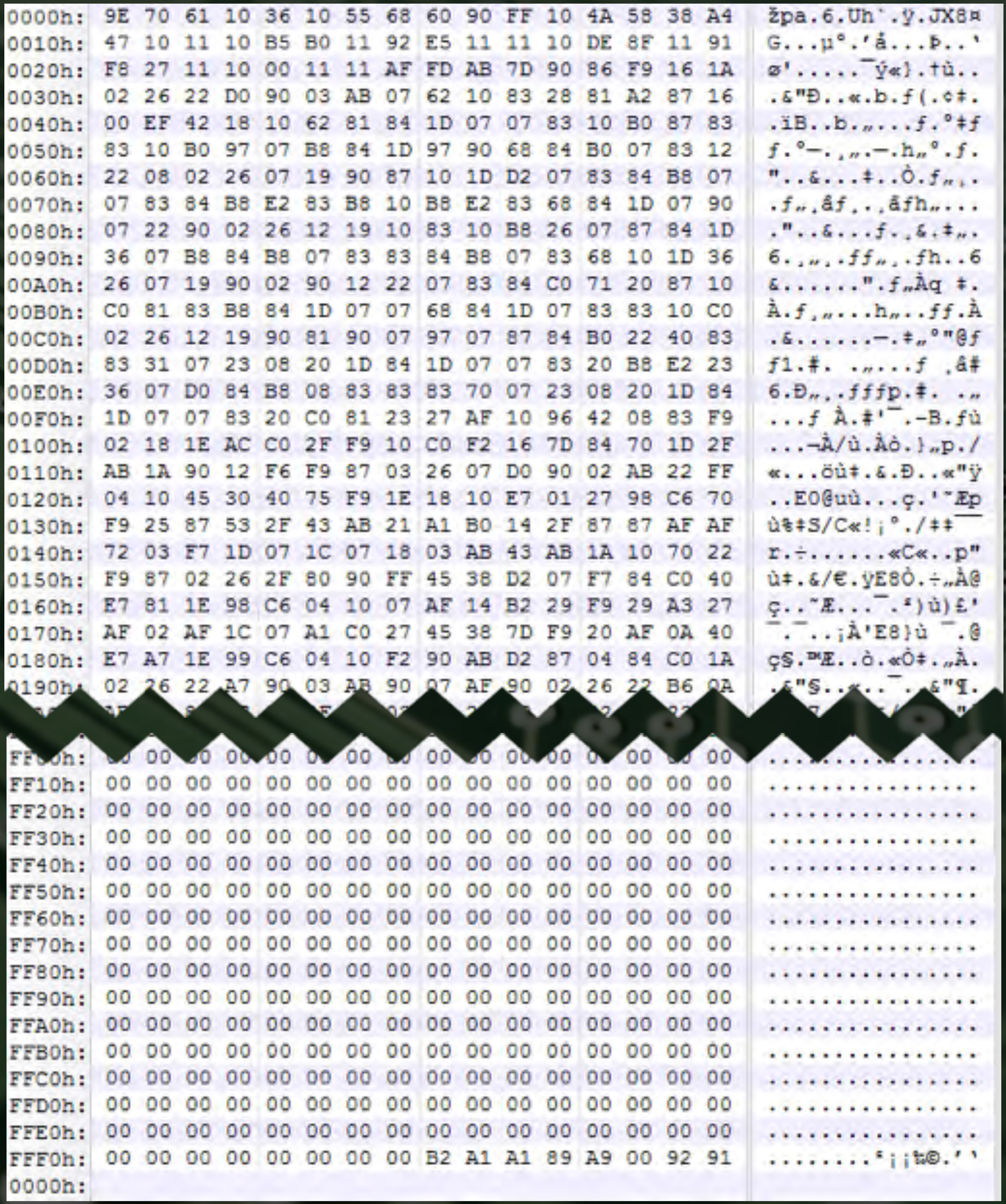
```
0130h: AA 76 D4 00 7C 10 F8 72 F2 E3 47 7C D4 D4 FC FC  ªvÔ.|.øròãG|ÔÔüü
0140h: 21 50 A4 4E 54 4F 54 4B 50 F8 10 F8 49 43 23 71  !P¤NTOTKPø.øIC#q
0150h: AA D4 51 75 7C D3 C3 AC 16 6B 81 54 A4 D7 93 13  ªÔQu|ÓÃ¬.k.T¤×“.
```

0x53⊕0x53= 0x00

```
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  SSSSSSSSáòòÚúSÁÂ
0000h:
```

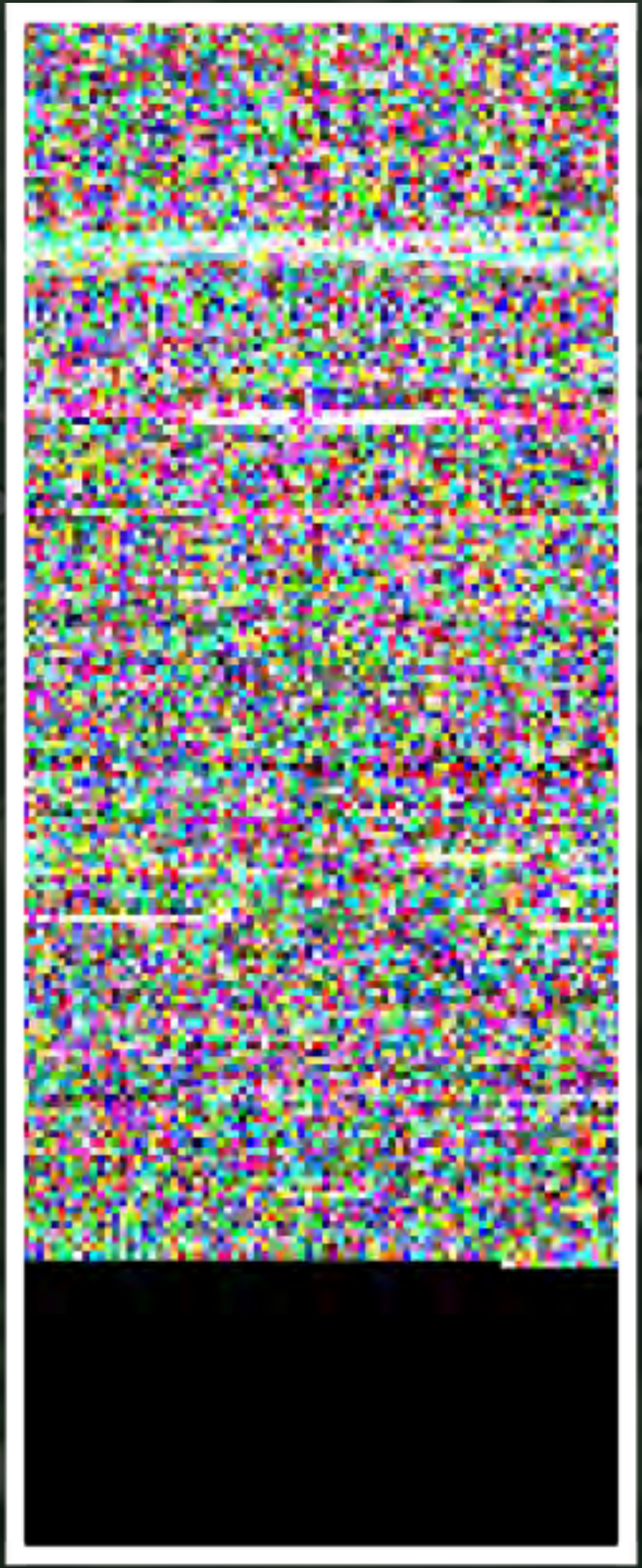


# ALLDONE!

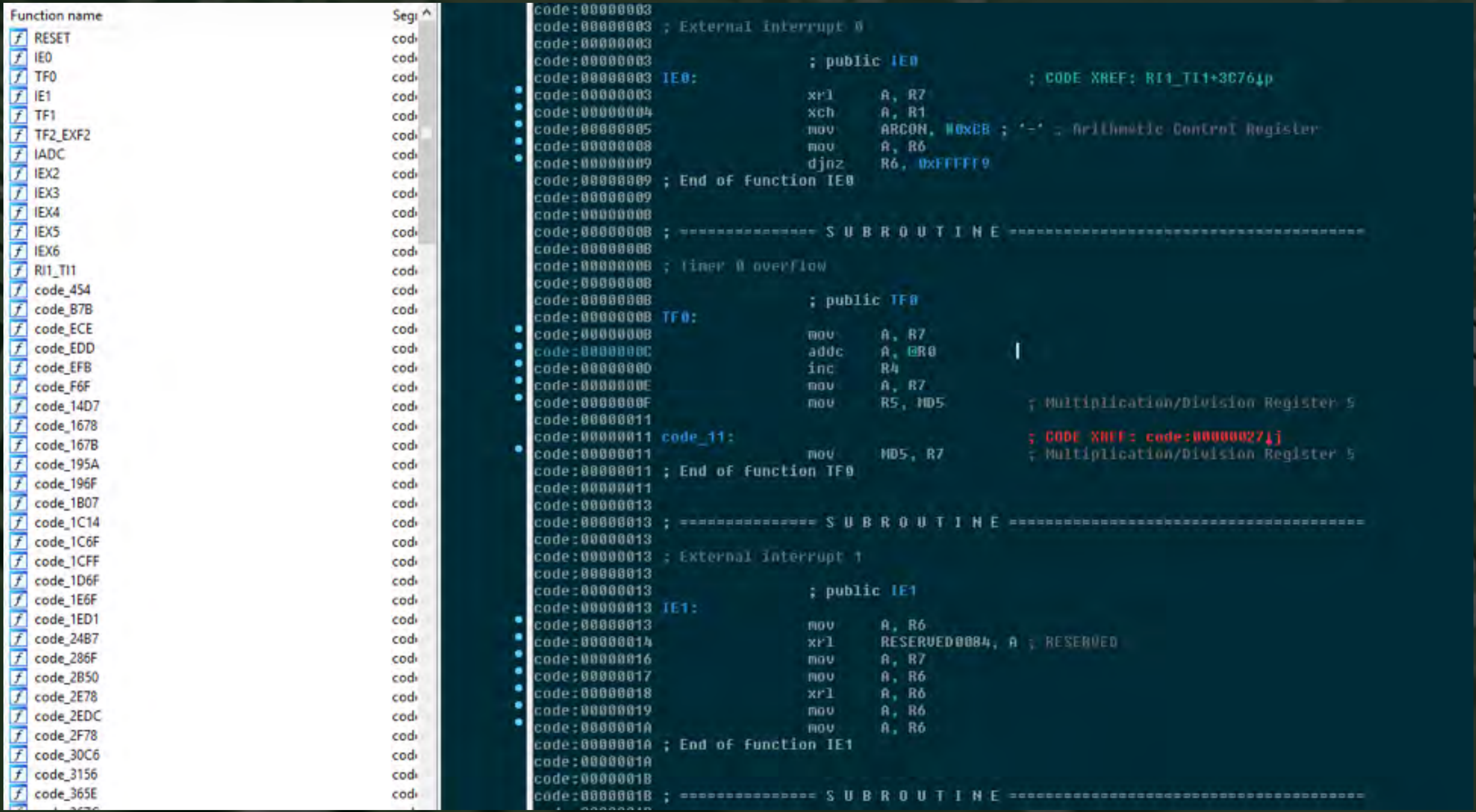


```
0000h: 9E 70 61 10 36 10 55 68 60 90 FF 10 4A 58 38 A4  žpa.6.Uh`.ÿ.JX8¤
0010h: 47 10 11 10 B5 B0 11 92 E5 11 11 10 DE 8F 11 91  G...µ°.'å...Þ..'
0020h: F8 27 11 10 00 11 11 AF FD AB 7D 90 86 F9 16 1A  ø'.....¯ý«}.†ù..
0030h: 02 26 22 D0 90 03 AB 07 62 10 83 28 81 A2 87 16  .&"Ð..«.b.ƒ(.¢‡.
0040h: 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:
```



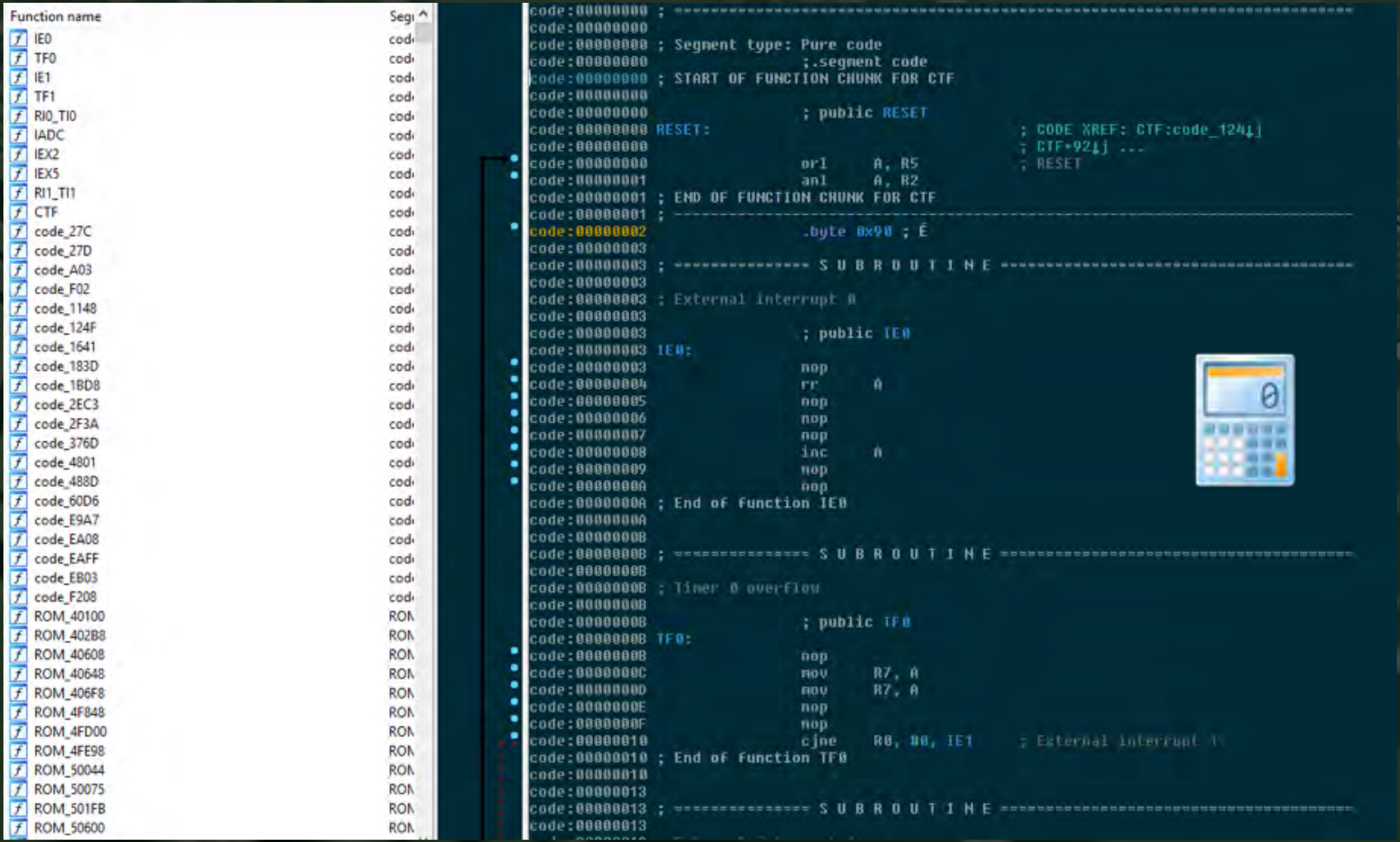
# 8051 ASSEMBLY?



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

```
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, 0xFFFFF9
code:00000009 ; End of function IE0
code:00000009
code:0000000B
code:0000000B ; =============== S U B R O U T I N E =======================================
code:0000000B
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: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
code:00000013 ; =============== S U B R O U T I N E =======================================
code:00000013
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 =======================================
```

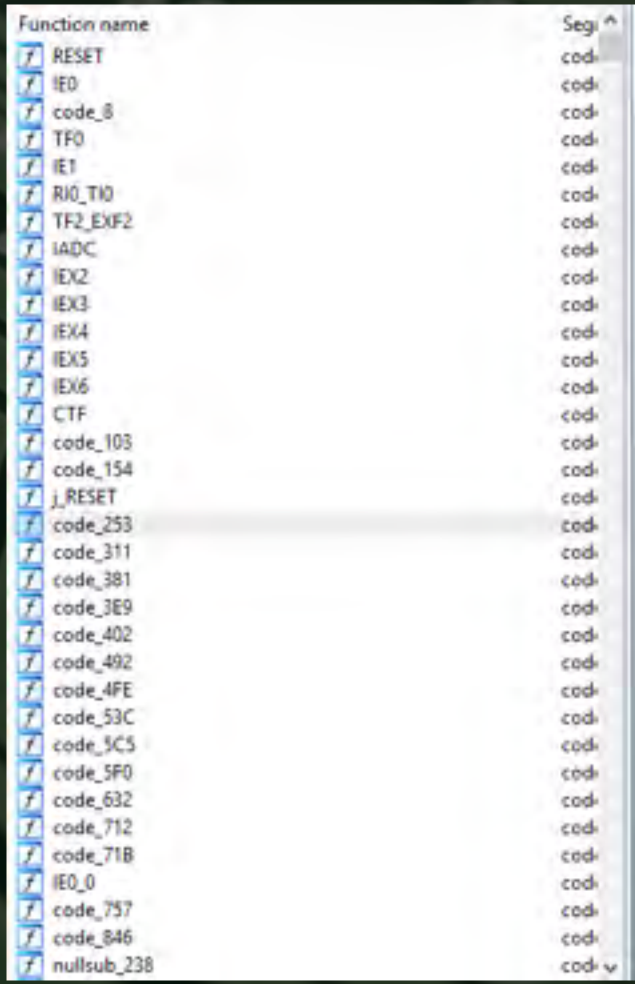
# 8051 ASSEMBLY?



| Function name | Segi |
|---|---|
| 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 | RO |
| ROM_402B8 | RO |
| ROM_40608 | RO |
| ROM_40648 | RO |
| ROM_406F8 | RO |
| ROM_4F848 | RO |
| ROM_4FD00 | RO |
| ROM_4FE98 | RO |
| ROM_50044 | RO |
| ROM_50075 | RO |
| ROM_501FB | RO |
| ROM_50600 | RO |

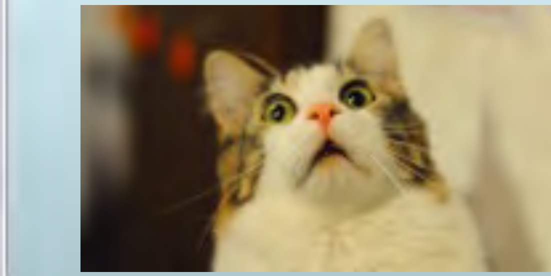
```
code:00000000 ; ===============================================================================
code:00000000
code:00000000 ; Segment type: Pure code
code:00000000                 ;.segment code
code:00000000 ; START OF FUNCTION CHUNK FOR CTF
code:00000000
code:00000000                 ; public RESET
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
code:00000003 ; =============== S U B R O U T I N E =======================================
code:00000003
code:00000003 ; External interrupt 0
code:00000003
code:00000003                 ; public IE0
code:00000003 IE0:
code:00000003                 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
code:0000000B
code:0000000B ; =============== S U B R O U T I N E =======================================
code:0000000B
code:0000000B ; Timer 0 overflow
code:0000000B
code:0000000B                 ; public TF0
code:0000000B TF0:
code:0000000B                 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
code:00000013
code:00000013 ; =============== S U B R O U T I N E =======================================
code:00000013
```

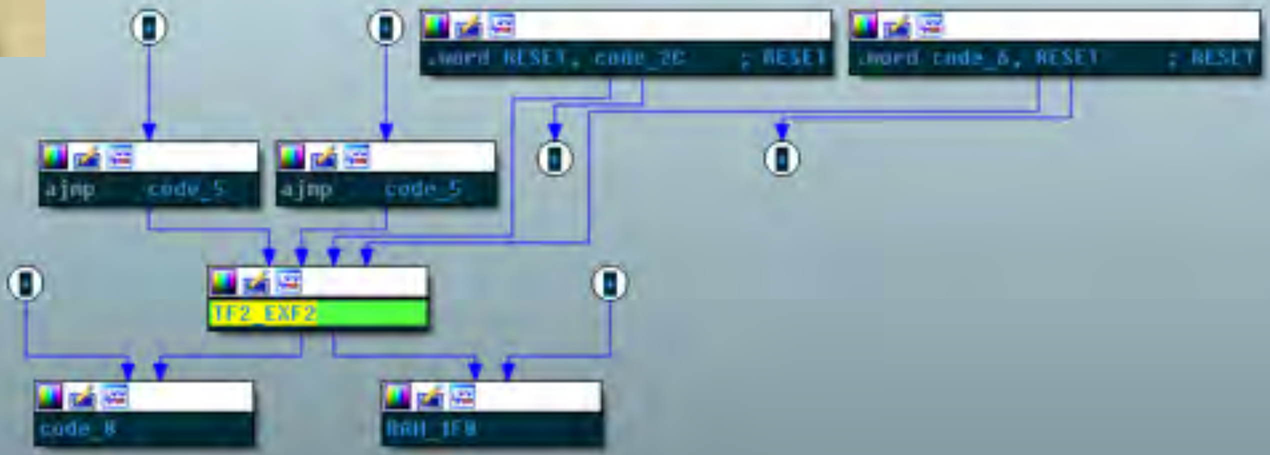
# 8051 ASSEMBLY?



| Function name | Segı |
|---|---|
| RESET | cod |
| IE0 | cod |
| code_8 | cod |
| TF0 | cod |
| IE1 | cod |
| RI0_TI0 | cod |
| TF2_EXF2 | cod |
| IADC | cod |
| IEX2 | cod |
| IEX3 | cod |
| IEX4 | cod |
| IEX5 | cod |
| IEX6 | cod |
| CTF | cod |
| code_103 | cod |
| code_154 | cod |
| j_RESET | cod |
| code_253 | cod |
| code_311 | cod |
| code_381 | cod |
| code_3E9 | cod |
| code_402 | cod |
| code_492 | cod |
| code_4FE | cod |
| code_53C | cod |
| code_5C5 | cod |
| code_5F0 | cod |
| code_632 | cod |
| code_712 | cod |
| code_71B | cod |
| IE0_0 | cod |
| code_757 | cod |
| code_846 | cod |
| nullsub_238 | cod |

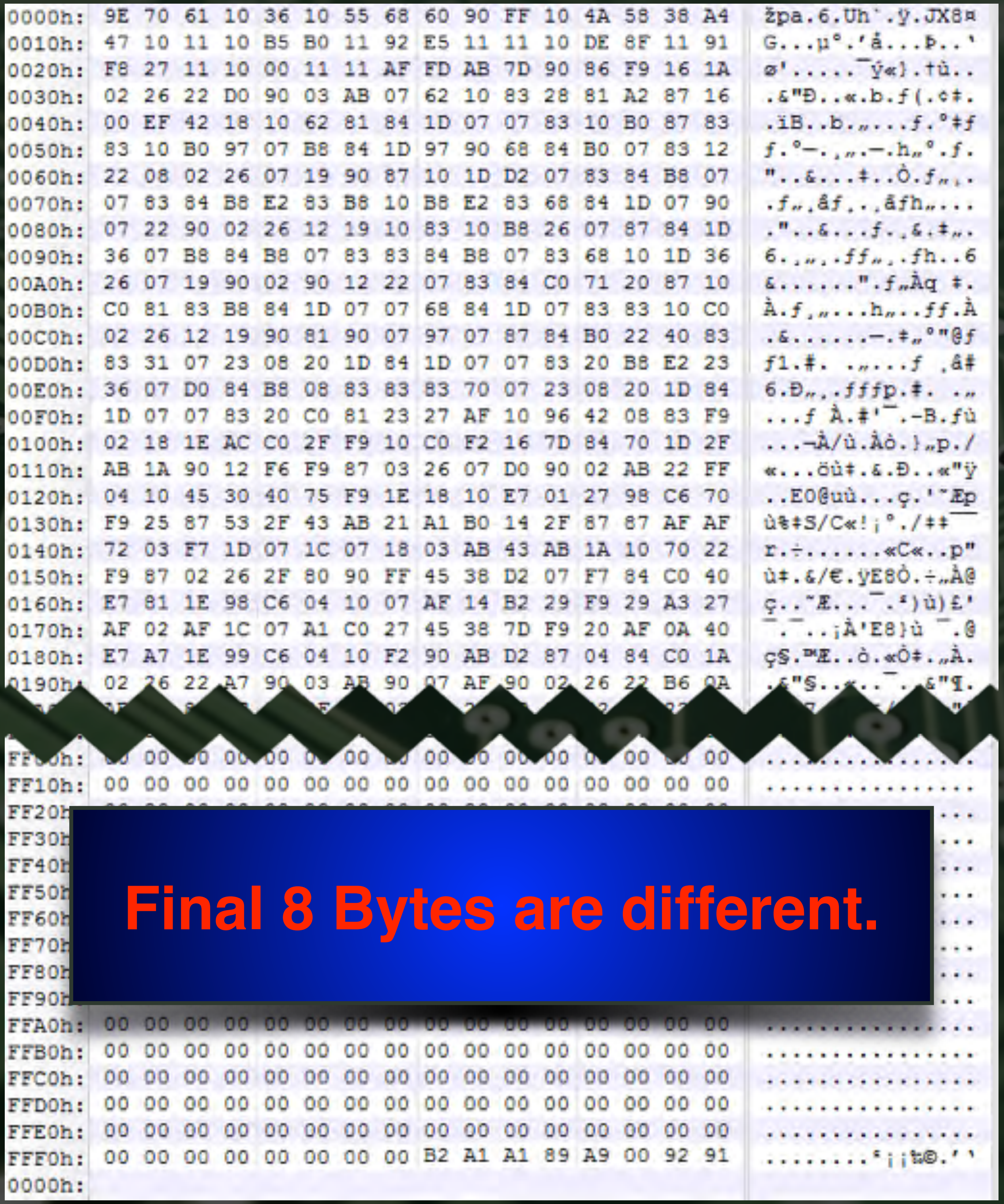
## EVERYTHING IS 8051!!!





```
.word RESET, code_2C     ; RESET
.word code_6, RESET      ; RESET
ajmp    code_5
ajmp    code_5
TF2_EXF2
code_8
RAM_1F8
```

# 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
FF30h
FF40h
FF50h
FF60h
FF70h
FF80h
FF90h
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.

# ACLUE?

- What does these last 8 bytes mean?
- Are they a clue left for use by a mad embedded developer?
- If we could just get some more data…

# FIRMWAREDIFFS!

- We have only analyzed a single firmware version.
- Perhaps other firmware versions could be insightful.

| 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 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 |

# APATTERN?

- Listing the binary values of these “patterns” from all firmware versions.

- If only these were ASCII values…

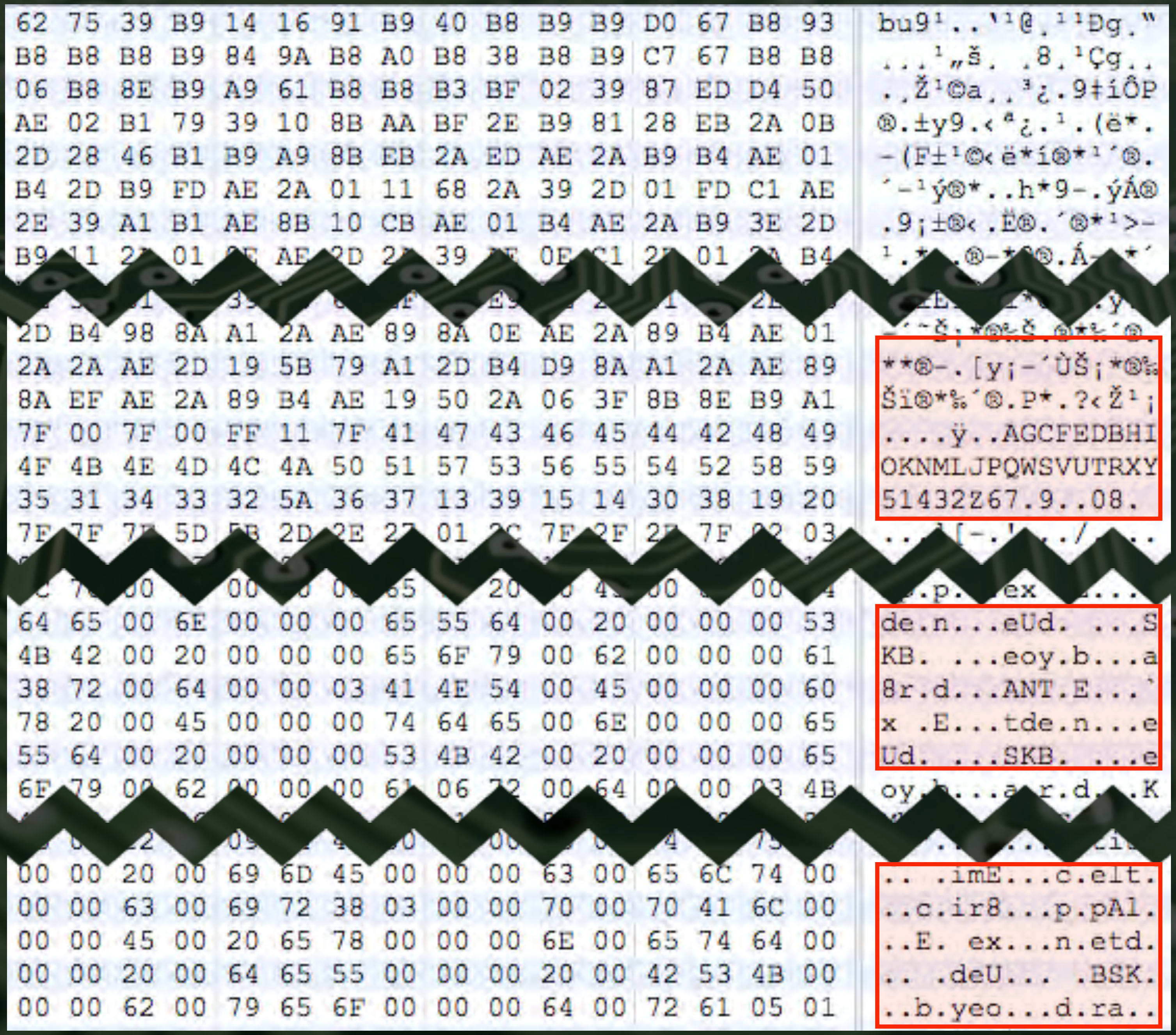
| Value | Hex | Binary |
|---|---|---|
| 1 | 0x89 | 10001001 |
| 2 | 0x91 | 10010001 |
| 3 | 0x99 | 10011001 |
| 4 | 0xA1 | 10100001 |
| 5 | 0xA9 | 10101001 |
| 6 | 0xB1 | 10110001 |
| 7 | 0xB9 | 10111001 |
| 8 | 0xC1 | 11000001 |
| 9 | 0xC9 | 11001001 |

# THEYCOULDBE!

- If we shift the bits 3 positions to the right.
- We get our ASCII values!

| Value | Hex | Binary | ROR 3 | ASCII |
|---|---|---|---|---|
| 1 | 0x89 | 10001001 | 00110001 | 1 |
| 2 | 0x91 | 10010001 | 00110010 | 2 |
| 3 | 0x99 | 10011001 | 00110011 | 3 |
| 4 | 0xA1 | 10100001 | 00110100 | 4 |
| 5 | 0xA9 | 10101001 | 00110101 | 5 |
| 6 | 0xB1 | 10110001 | 00110110 | 6 |
| 7 | 0xB9 | 10111001 | 00110111 | 7 |
| 8 | 0xC1 | 11000001 | 00111000 | 8 |
| 9 | 0xC9 | 11001001 | 00111001 | 9 |

# STRINGS?



```
62 75 39 B9 14 16 91 B9 40 B8 B9 B9 D0 67 B8 93   bu9¹..'¹@¸¹¹Ðg¸"
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¸¸³¿.9‡íÔP
AE 02 B1 79 39 10 8B AA BF 2E B9 81 28 EB 2A 0B   ®.±y9.‹ª¿.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>-
```

```
2D B4 98 8A A1 2A AE 89 8A 0E AE 2A 89 B4 AE 01
2A 2A AE 2D 19 5B 79 A1 2D B4 D9 8A A1 2A AE 89   **®-.[y¡-´ÙŠ¡*®‰
8A EF AE 2A 89 B4 AE 19 50 2A 06 3F 8B 8E B9 A1   Šï®*‰´®.P*.?‹Ž¹¡
7F 00 7F 00 FF 11 7F 41 47 43 46 45 44 42 48 49   ....ÿ..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.
```

```
64 65 00 6E 00 00 00 65 55 64 00 20 00 00 00 53   de.n...eUd. ...S
4B 42 00 20 00 00 00 65 6F 79 00 62 00 00 00 61   KB. ...eoy.b...a
38 72 00 64 00 00 03 41 4E 54 00 45 00 00 00 60   8r.d...ANT.E...`
78 20 00 45 00 00 00 74 64 65 00 6E 00 00 00 65   x .E...tde.n...e
55 64 00 20 00 00 00 53 4B 42 00 20 00 00 00 65   Ud. ...SKB. ...e
```

```
00 00 20 00 69 6D 45 00 00 00 63 00 65 6C 74 00   .. .imE...c.elt.
00 00 63 00 69 72 38 03 00 00 70 00 70 41 6C 00   ..c.ir8...p.pAl.
00 00 45 00 20 65 78 00 00 00 6E 00 65 74 64 00   ..E. ex...n.etd.
00 00 20 00 64 65 55 00 00 00 20 00 42 53 4B 00   .. .deU... .BSK.
00 00 62 00 79 65 6F 00 00 00 64 00 72 61 05 01   ..b.yeo...d.ra..
```

# RESHUFFLE

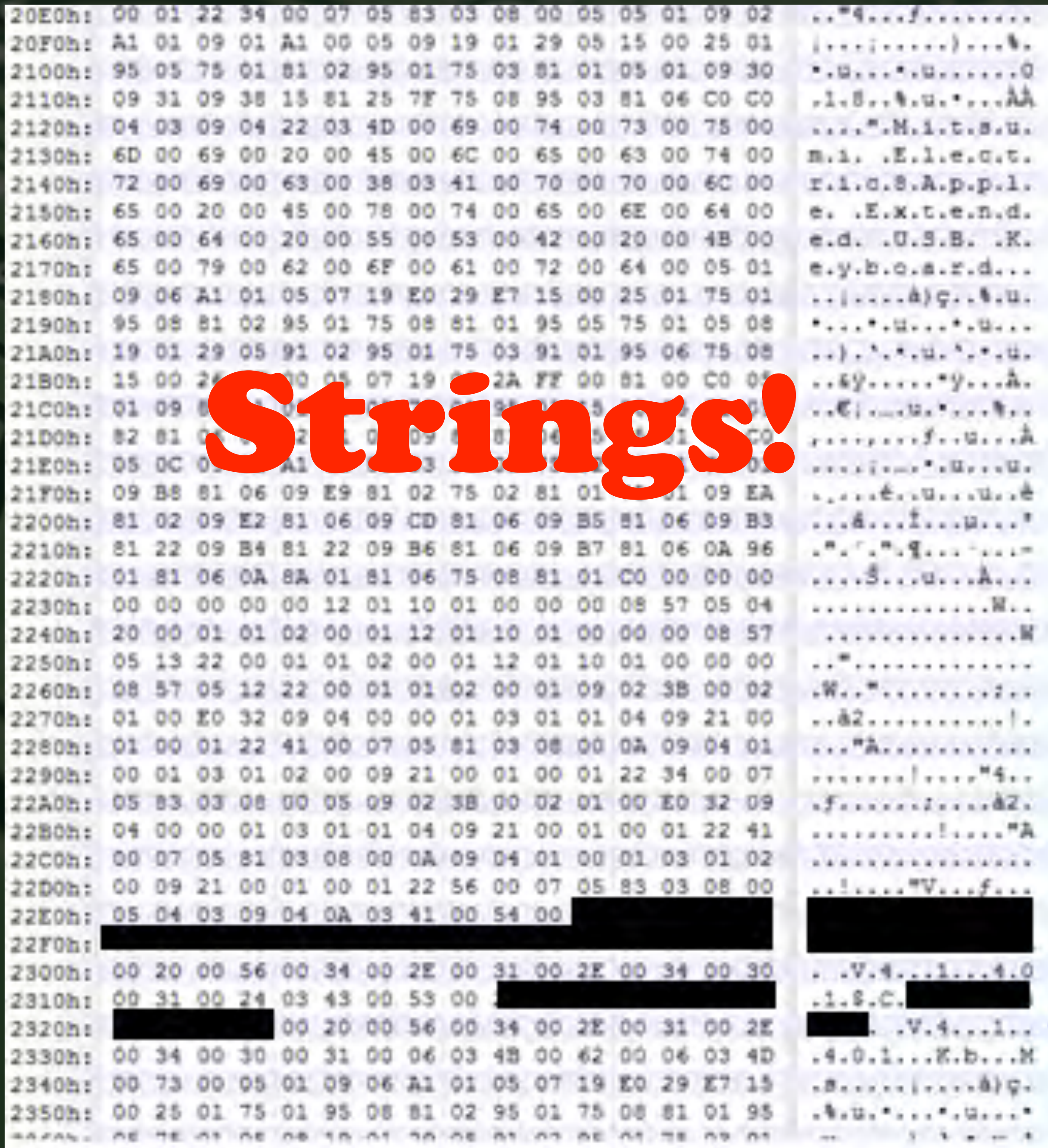
| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| A | G | C | F | E | D | B | H | I | O | K | N | M | L | J | P | Q | W | S | V | U | T | R | X |

# 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |

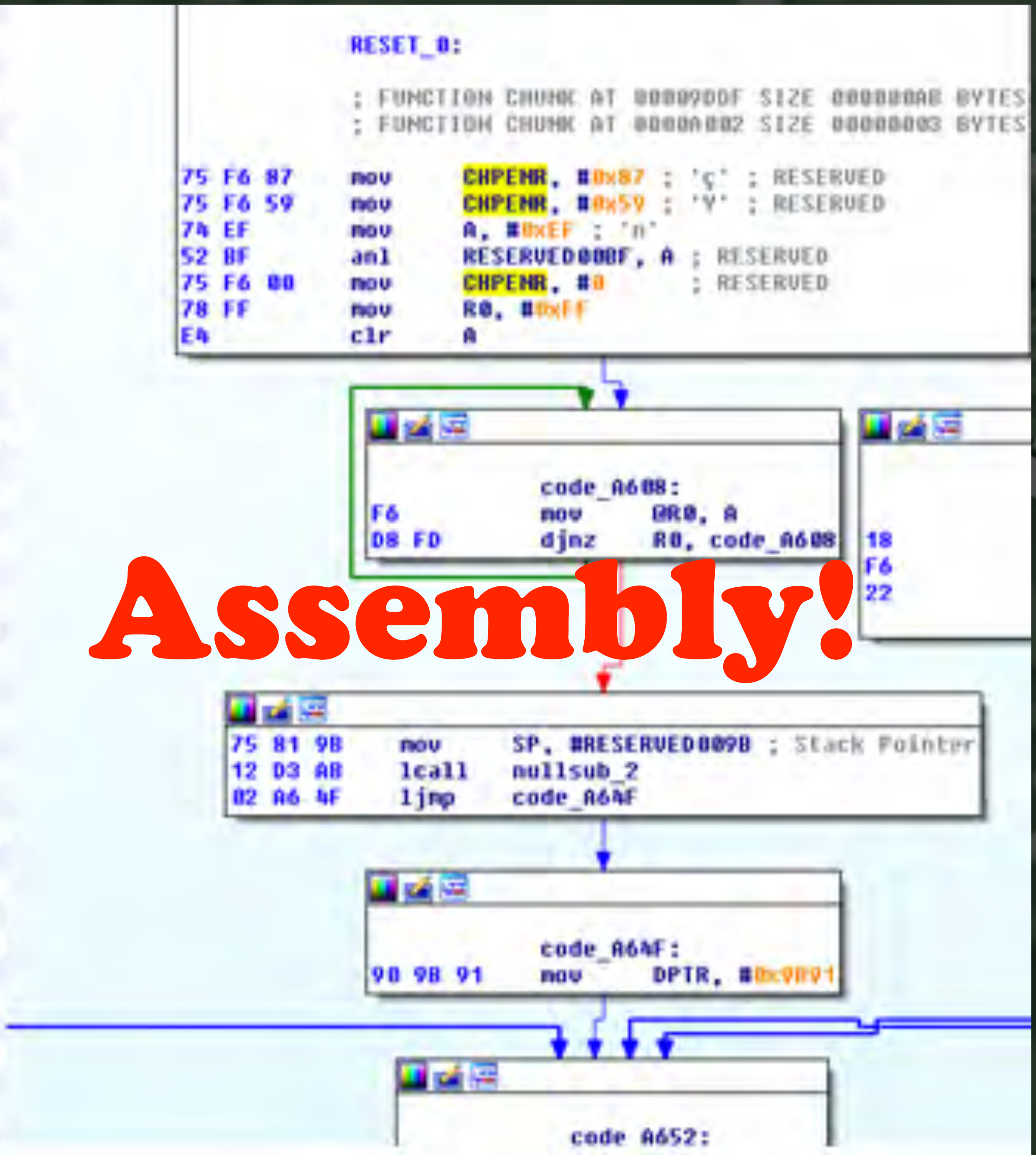
| Position | Original |
|---|---|
| 1 | 1 |
| 2 | 7 |
| 3 | 3 |
| 4 | 6 |
| 5 | 5 |
| 6 | 4 |
| 7 | 2 |
| 8 | 8 |

# SUCCESS!!!



```
20E0h: 00 01 22 34 00 07 05 83 03 08 00 05 05 01 09 02  .."4...ƒ........
20F0h: A1 01 09 01 A1 00 05 09 19 01 29 05 15 00 25 01  ¡...¡.....)...%.
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  .1.8..%.u.•...ÀÀ
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.8.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  ..¡....à)ç..%.u.
2190h: 95 08 81 02 95 01 75 08 81 01 95 05 75 01 05 08  •...•.u...•.u...
21A0h: 19 01 29 05 91 02 95 01 75 03 91 01 95 06 75 08  ..).'.•.u.'.•.u.
21B0h: 15 00 [illegible] 05 07 19 [illegible] 2A FF 00 81 00 C0 05  ..&ÿ.....*ÿ...À.
21C0h: 01 09 [illegible]  ..€¦.…..u.•...‰..
21D0h: 82 81 [illegible] C0  ,...,...ƒ..u...À
21E0h: 05 0C [illegible] A1 [illegible]  ....¦.—.•.u...u.
21F0h: 09 B8 81 06 09 E9 81 02 75 02 81 01 [illegible] 01 09 EA  ..,...é..u...u..ê
2200h: 81 02 09 E2 81 06 09 CD 81 06 09 B5 81 06 09 B3  ...â...Í...µ...³
2210h: 81 22 09 B4 81 22 09 B6 81 06 09 B7 81 06 0A 96  ."..´."..¶...·...–
2220h: 01 81 06 0A 8A 01 81 06 75 08 81 01 C0 00 00 00  ....Š...u...À...
2230h: 00 00 00 00 00 12 01 10 01 00 00 00 08 57 05 04  .............W..
2240h: 20 00 01 01 02 00 01 12 01 10 01 00 00 00 08 57   ..............W
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  ..à2..........!.
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  .ƒ......;....à2.
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...ƒ...
22E0h: 05 04 03 09 04 0A 03 41 00 54 00 [redacted]
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 [redacted]  .1.$.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  .s.....¡....à)ç.
2350h: 00 25 01 75 01 95 08 81 02 95 01 75 08 81 01 95  .%.u.•...•.u...•
```

Strings!



```
                RESET_0:

                ; FUNCTION CHUNK AT 00009DDF SIZE 000000AB BYTES
                ; FUNCTION CHUNK AT 0000A002 SIZE 00000003 BYTES

75 F6 87        mov     CHPENR, #0x87 ; 'ç' ; RESERVED
75 F6 59        mov     CHPENR, #0x59 ; 'Y' ; RESERVED
74 EF           mov     A, #0xEF ; 'n'
52 BF           anl     RESERVED00BF, A ; RESERVED
75 F6 00        mov     CHPENR, #0      ; RESERVED
78 FF           mov     R0, #0xFF
E4              clr     A

                code_A608:
F6              mov     @R0, A
D8 FD           djnz    R0, code_A608

18
F6
22

75 81 9B        mov     SP, #RESERVED009B ; Stack Pointer
12 D3 AB        lcall   nullsub_2
02 A6 4F        ljmp    code_A64F

                code_A64F:
90 9B 91        mov     DPTR, #0x9B91

                code_A652:
```

Assembly!

# 8051FUN

- We can now design our own “custom” firmware-upgrade utility.
- However, we do need a basic understanding of 8051 Assembly!

# 8051REVIEW

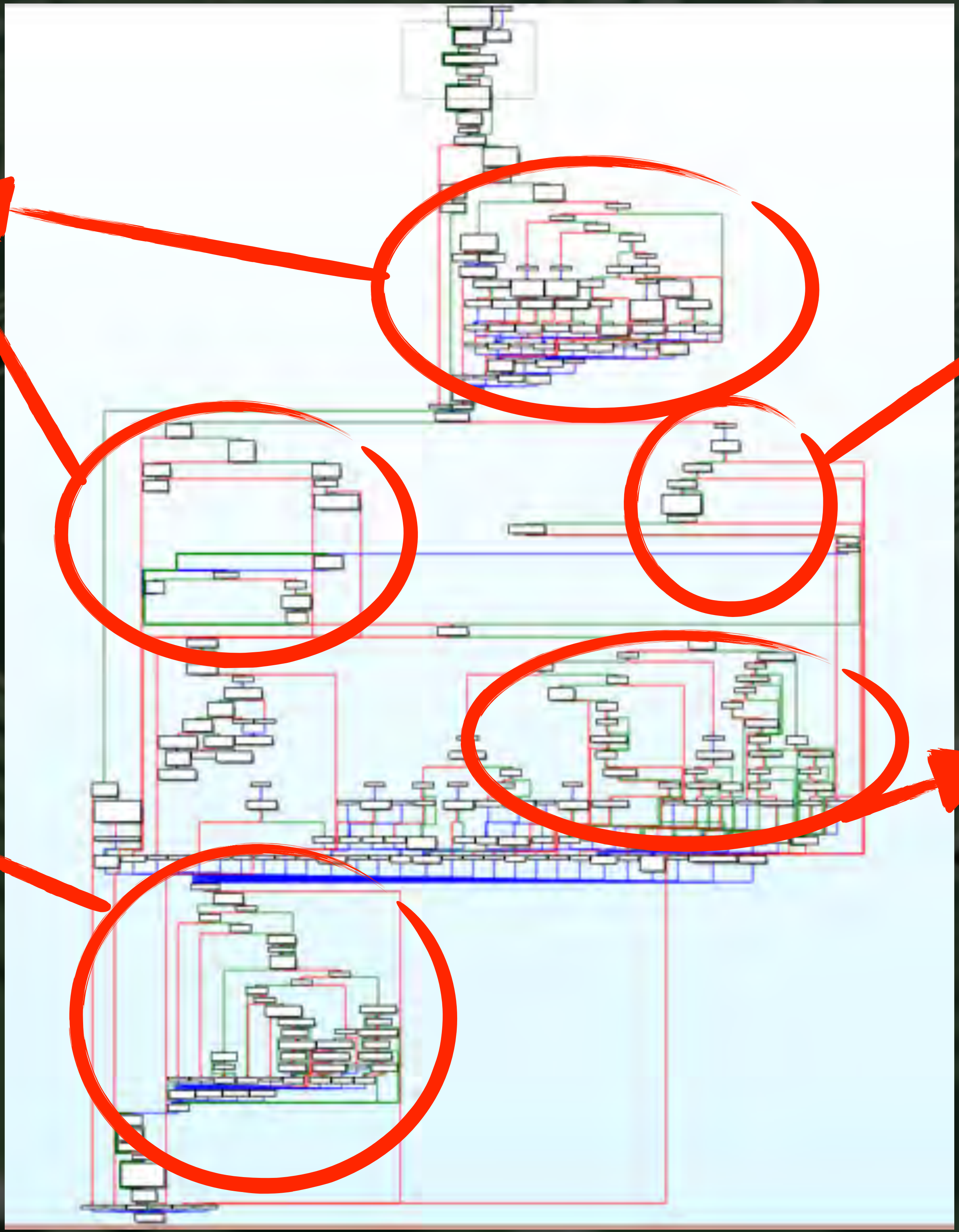
+ Only 255 OP-Codes, and ~40 Instructions.

- Functions are not *really* functions.

- Just a single memory access register.

- Registers keep on changing for some reason.

# KVMLOGIC



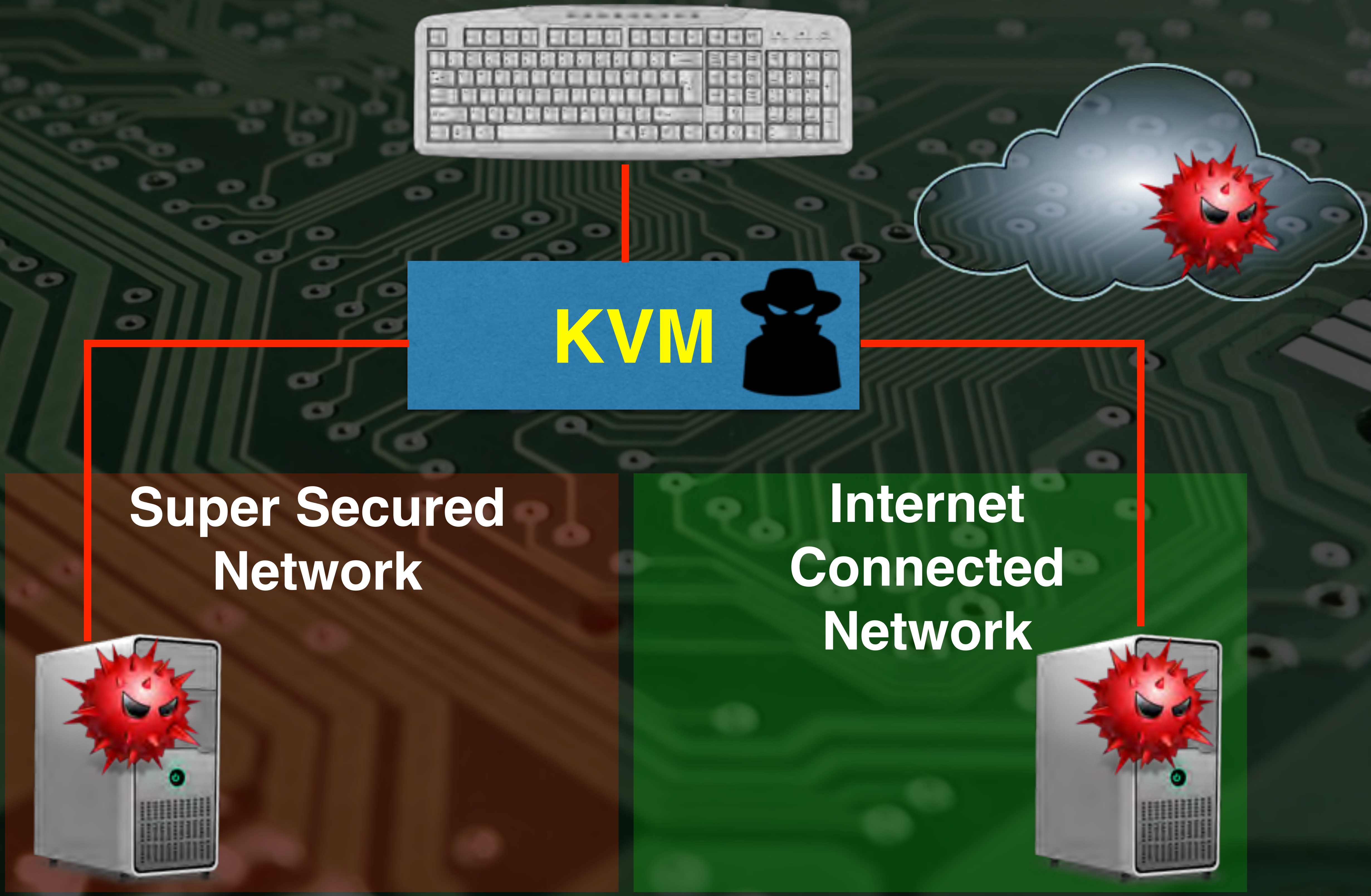
Keyboard Emulation

HID Parsing

Keyboard LEDs Control

Hotkeys Handling

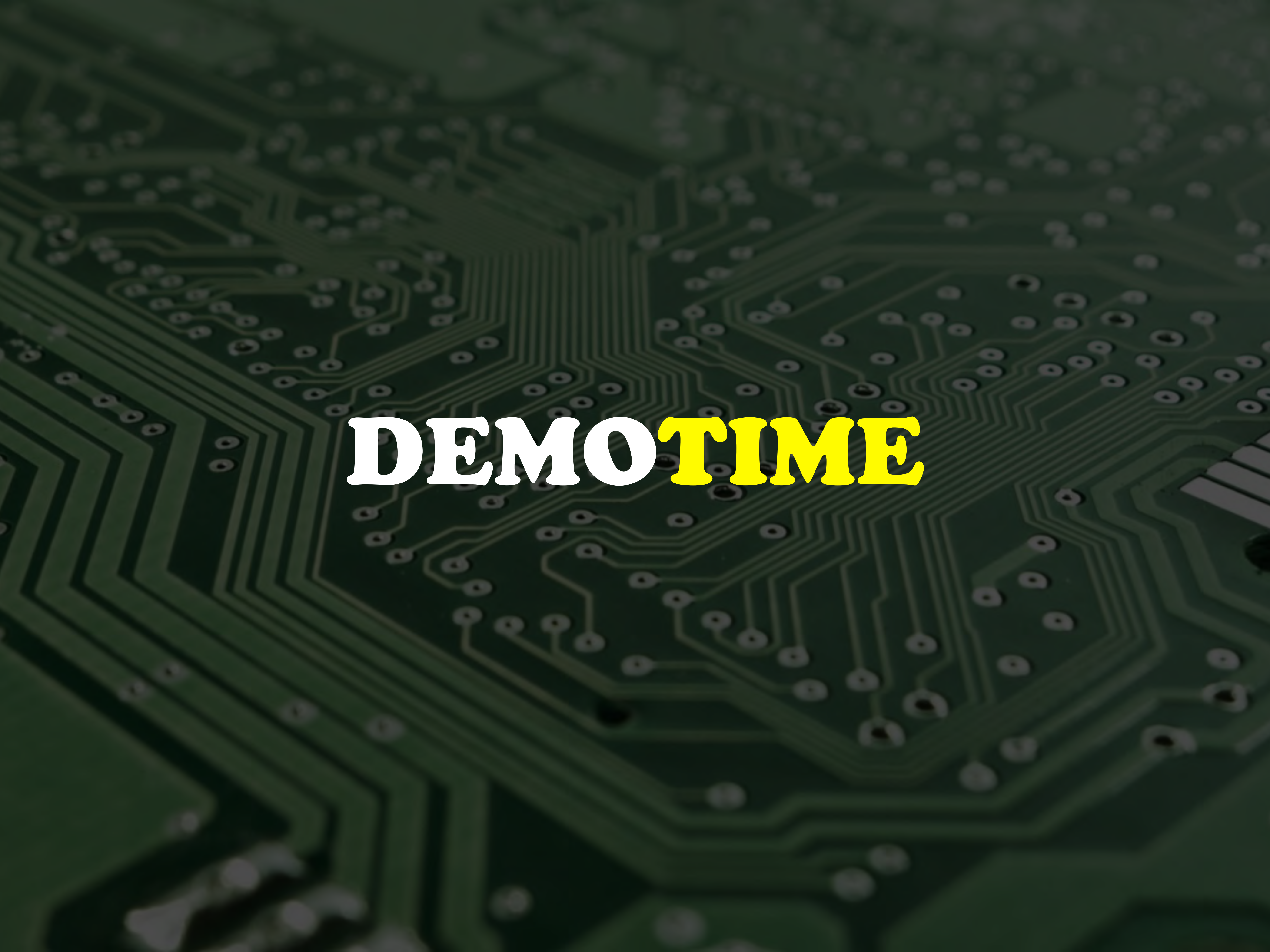
# MALKVM



KVM

Super Secured Network

Internet Connected Network



# DEMOTIME