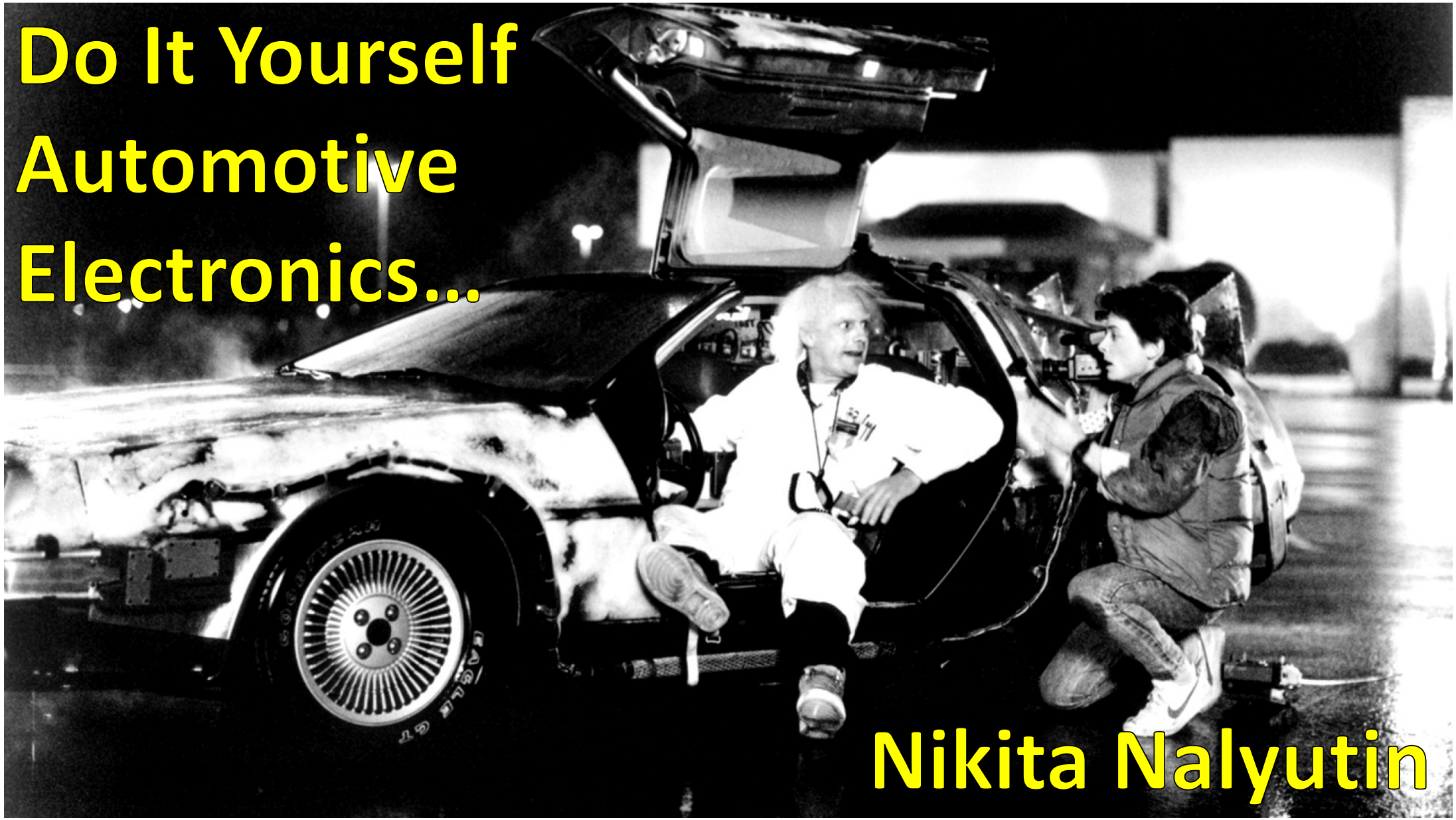

Do It Yourself
Automotive
Electronics…
Nikita Nalyutin


… that brings
some fun


Here
it comes
MERCURY


Once upon
a time...
FM2 94.9
10:20
SE
EXT TEMP
23
PASSENGER AIRBAG OFF
LOAD
EJECT
1
2
3
4
5
6
DIRECT
7
8
9
0
CLOCK
SCAN
SOUND
VOL
TUNE


... it was a boring FDIM*...
SE
MERCURY MARINER
13:44
*Ford Display Interface Module

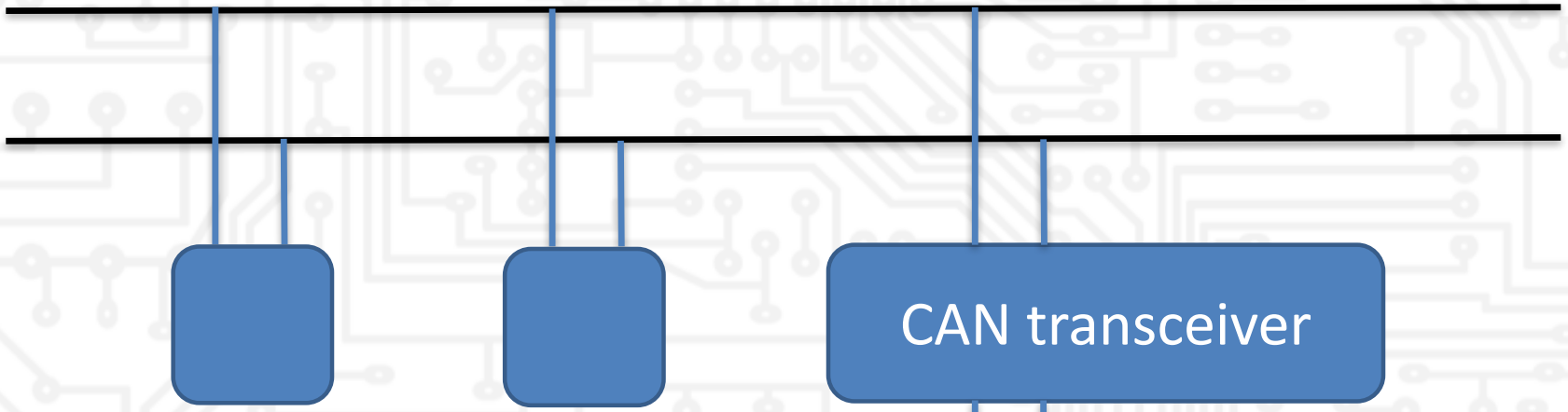

...who wanted
to be cool
STATS
CRIPPLED
RAD
EFF

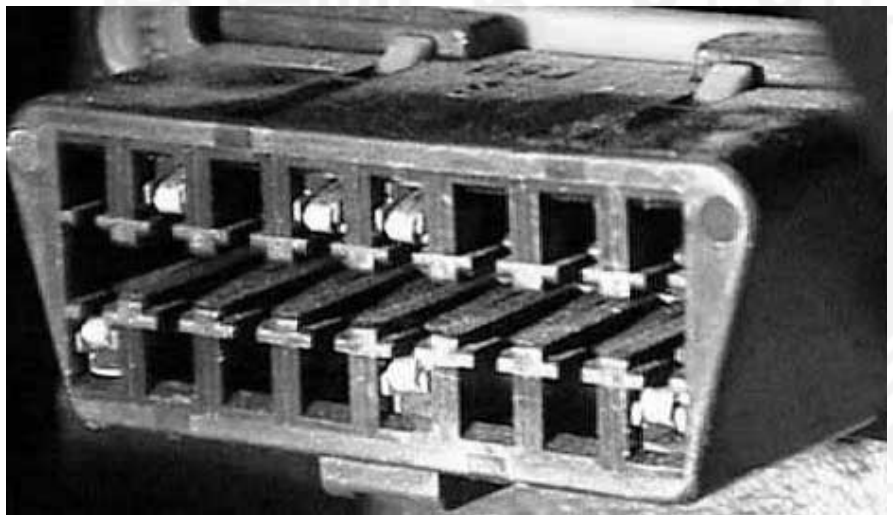
Own display

VS.

Head unit simulation

CAN bus





```
22f | 31 39 42 37 35 42 4B 00
```

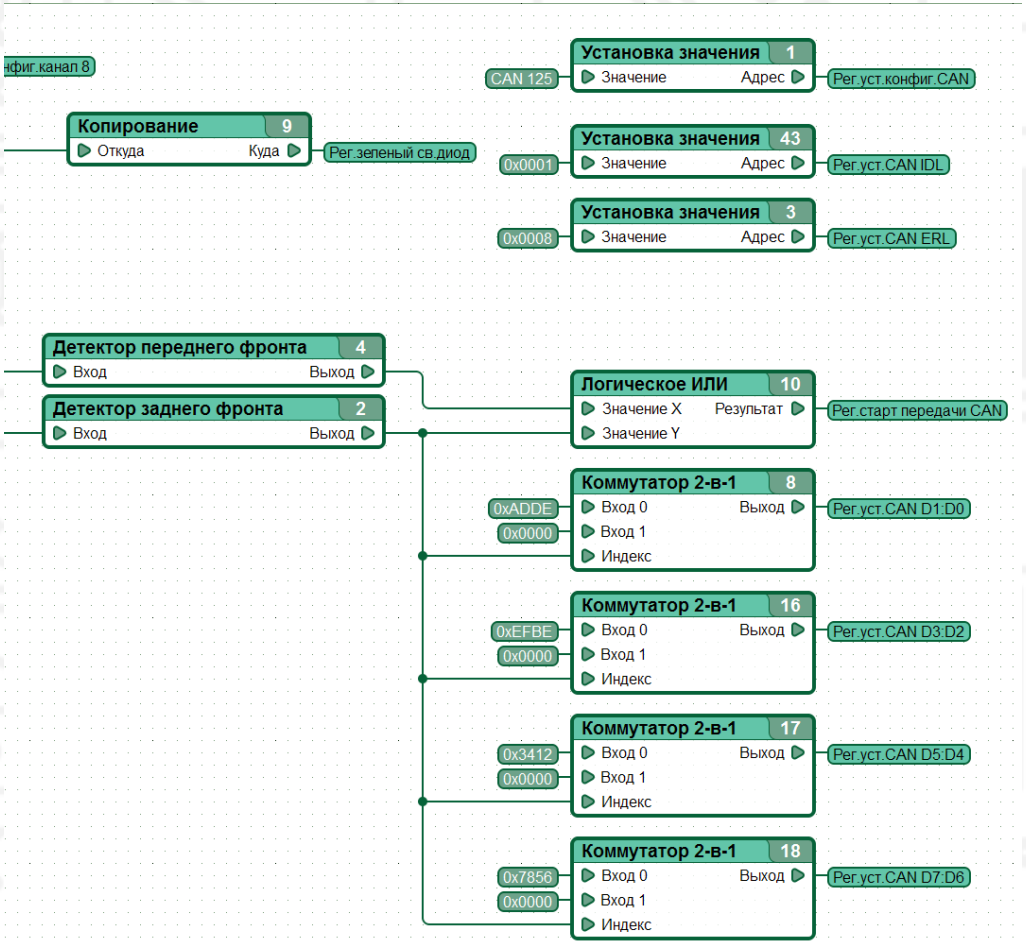
~ 10 USD

How to hook up: ELM327


```
>atma
7F F0 FF EF FE FF EF FE <DATA ERROR
00 00 00 00 22 50 00 00
C1E
0: 17 78 17 70 7E EA
40 00 00 00 00 00 00 00 <DATA ERROR
7: 10 0F 02 6F 00 00 00
00 56 00 00 00 00 00 00
7F F0 FF EF FE FF EF FE <DATA ERROR
00 00 00 00 00 00 00 00
00 00 00 00 EE 40 00 42
5C 12 00 <DATA ERROR
C1A
0: 17 72 17 50 7E F4
7F F0 FF EF FE FF EF FE <DATA ERROR
00 00 00 00 54 50 00 00
C0C
BUFFER FULL
```

How to hook up: Canny

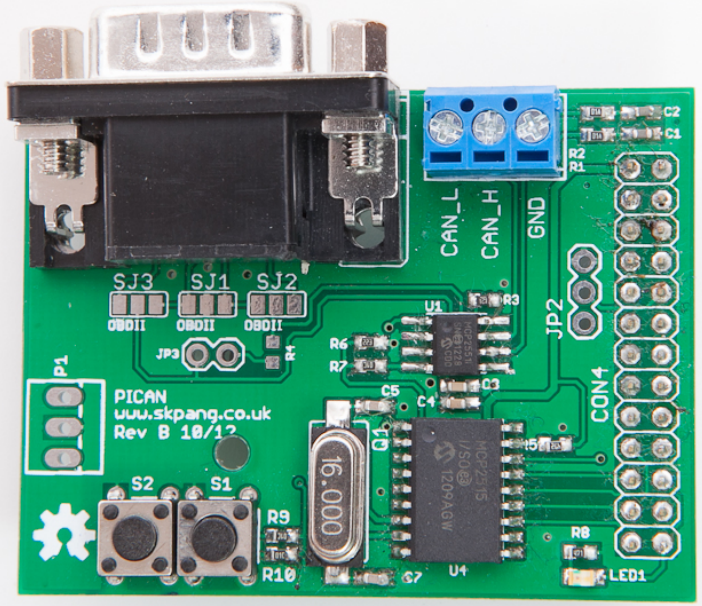
~ 50 USD



http://www.canny.ru

~ 30 GBP

How to hook up: PiCAN



After **long work and a lot of pain** I managed to set up can communication on Raspberry Pi. Since i experienced lack of simple help here in this discussion i want to share my knowledge with you. Here is what i did:

<bla-bla-bla-bla>

... and this is it! CanBus communication now works like a charm

https://www.raspberrypi.org/forums/viewtopic.php?f=44&t=7027

~ 25 USD

How to hook up: CAN Bus Shield

Lots of docs

- Schematic
- Eagle Files
- Datasheet (MCP2515)
- Datasheet (MCP2551)
- Hookup Guide
- OBD-II Guide
- GitHub (Design Files)
- GitHub (Library & Example Code)
- Product Video

https://www.sparkfun.com/products/13262

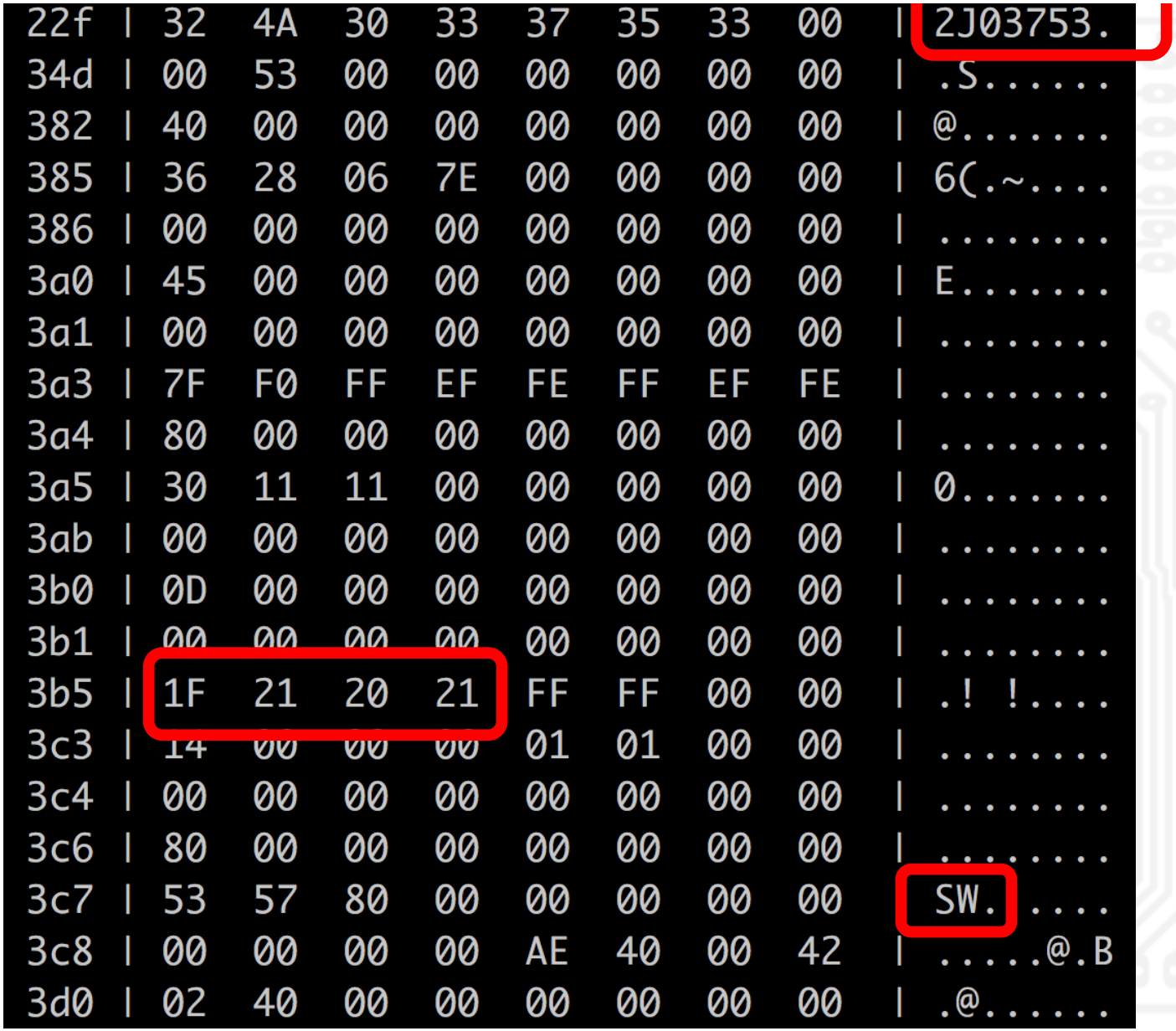
~ 3 USD

How to hook up: China wonder

MCP2515	Arduino Nano
INT	D2
SCK	D13
SI	D11
SO	D12
CS	D10
GND	GND
VCC	+5V

AliExpress: search “mcp2515 module”


China - think different!
Frequencies do not match!
8 MHz here
16 MHz here
8.000
M1600CB
520-030-R
#define MCP_16MHz_500kBPS_CFG1 (0x00)
#define MCP_16MHz_500kBPS_CFG2 (0xF0)
#define MCP_16MHz_500kBPS_CFG3 (0x86)
Standard Arduino libraries are for 16 MHz
PICAN
www.skpang.co.uk
Rev B 10/12
NiRen



Reversing tools: eyes

You see here:

- **Part of VIN**
- **Tires pressure**
- **Compass**

Maybe smth else?

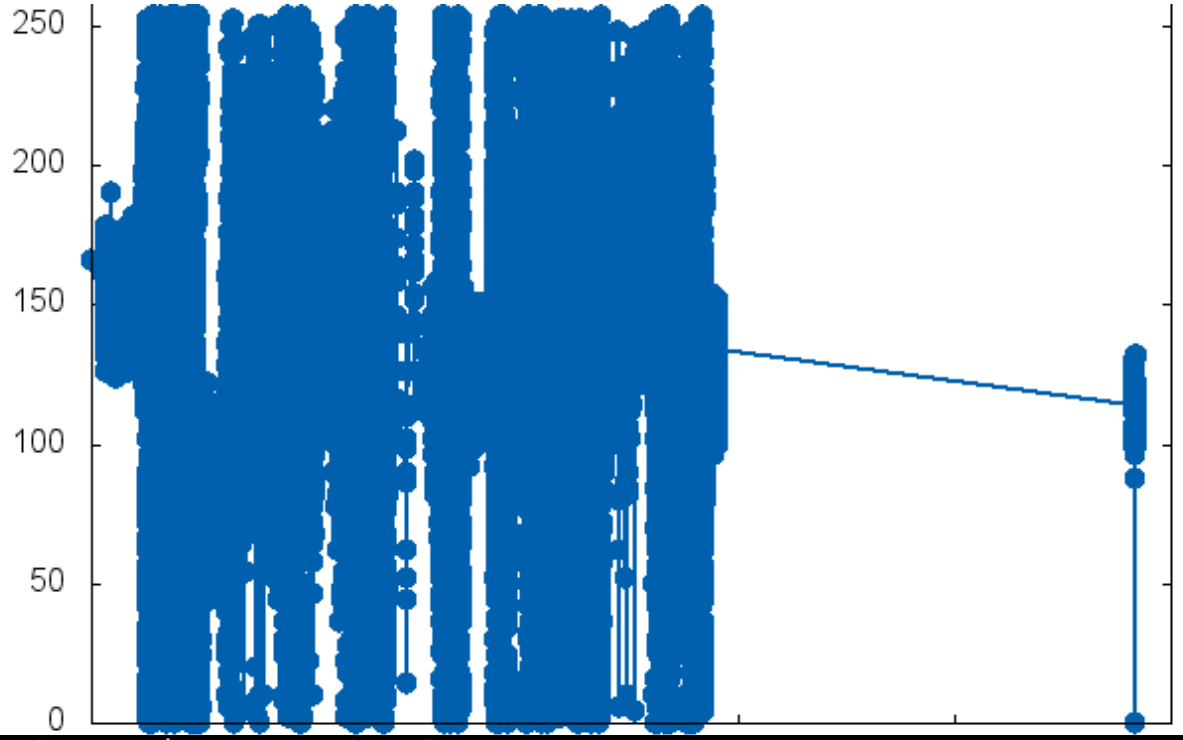
```
bash-3.2$ cat "CoolTerm Capture 2015-12-03 21-55"\
> | cut -f2 -d\  | sort | uniq
0x1C
0x22F
0x34D
0x382
0x383
0x385
0x386
0x3A0
0x3A1
0x3A3
0x3A4
0x3A5
0x3AB
0x3B0
0x3B1
0x3B5
0x3C3
```

Reversing tools: diff

Connect
Dump

Disconnect
Dump

Diff
Compare




```
bash-3.2$ cat makeplot
#!/bin/bash
gnuplot -e "filename='$1';ofilename='$1.png'" gnu.plot

bash-3.2$ cat gnu.plot
set terminal 'png'
set output ofilename
set style line 1 lc rgb '#0060ad' lt 1 lw 2 pt 7 ps 1.5
plot filename with linespoints ls 1
```

Reversing tools: plots

Dump

Draw plots (gnuplot/Excel)

Hard thinking

Here we have steering wheel position (one of 3 values)

```
bash-3.2$ cat ms-can-unique.txt
0x136
0x2DB - SYNC buttons?
0x22F - VIN
0x34D - ??? 2nd byte, irregular jigsaw values 69-88
0x382 - no changes
0x383 - turn signal
0x385 - maybe HVAC buttons?
0x386 - no changes, always zero
0x3A0 - ignition swith, braking
0x3A1 - HVAC?
0x3A3 - no changes
0x3A4 - HVAC?
0x3A5 - no changes
0x3AB - instrument illumination level
0x3B0 - transmission selector
0x3B1 - doors
0x3B5 - TPMS
0x3C3 - braking
```

Reversing tools: aggregate

Sending CAN messages

Message sequences

- start sequence
- heartbeat
- regular data
- irregular data

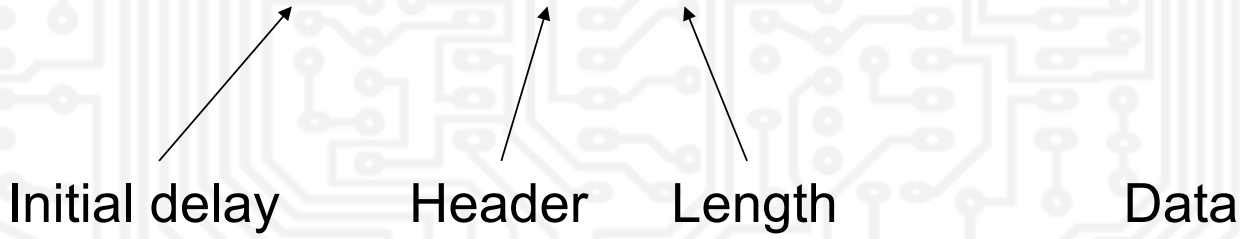
Message data structure

CANMessage(uint32_t **started**, uint32_t **delayed**, uint32_t **repeated**,
uint32_t **header**, byte **_len**, byte **d[8]**)

Message sending: CAN.sendMsgBuf(header, 0, len, data[8]);

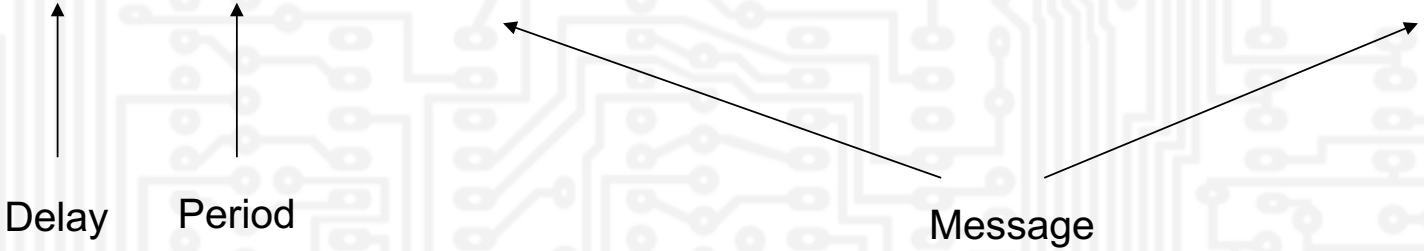
FDIM start sequence

```
void initStartMessages()
{
s[0].set( 0, 100, 0, 0x50c, 3, 0x0C,0x01,0x00,0x00,0x00,0x00,0x00,0x00 );
s[1].set( 0, 250, 0, 0x3e8, 8, 0x00,0x00,0x29,0x00,0x00,0x00,0x00,0x00 );
s[2].set( 0,  50, 0, 0x3ef, 8, 0x32,0x32,0x32,0x32,0x03,0x00,0x00,0x00 );
s[3].set( 0,  50, 0, 0x3f2, 8, 0xFF,0xFF,0xFF,0xFF,0xFF,0x60,0x00,0x00 );
s[4].set( 0, 100, 0, 0x50c, 3, 0x01,0x02,0x00,0x00,0x00,0x00,0x00,0x00 );
s[5].set( 0,  50, 0, 0x3f2, 8, 0x00,0x00,0xFF,0xFF,0xFF,0xF0,0x00,0x00 );
s[6].set( 0,  50, 0, 0x3f1, 8, 0xF5,0x90,0x00,0x00,0x00,0x00,0x00,0x00 );
s[7].set( 0, 100, 0, 0x50c, 3, 0x01,0x02,0x00,0x00,0x00,0x00,0x00,0x00 );
}
```



FDIM heartbeat

```
void initCycleMessages()
{
c[0].set(0,  0,  500, 0x50c, 3, 0x11,0x02,0x00,0xBE,0xBE,0xBE,0xBE,0xBE );
c[1].set(0,400, 1000, 0x3e8, 8, 0x0F,0x00,0x29,0x04,0x00,0x00,0x00,0x00 );
c[2].set(0,450, 1000, 0x3ef, 8, 0x32,0x32,0x32,0x32,0x03,0x00,0x00,0x20 );
c[3].set(0,500, 1000, 0x3f2, 8, 0x12,0x01,0xFF,0xFF,0xFF,0xF0,0x00,0x00 );
}
```



FDIM printing text

```
void initTextMessages()
{
t[ 0].set( 1000,  0, 500, 0x336,8, 0x03, 0x01,0x0A,0x01,0xFE,0x00,0x00,0x00 );
t[ 1].set( 1000, 50, 500, 0x324,8, 0x01, 0x01,0x02,0x00,0x00,0x00,0x00,0x00 );
t[ 2].set( 1000,100, 500, 0x337,8, 0x06, 0x20, ' ', '@', ' ', '@', ' ',0x00 );
t[ 3].set( 1000,200, 500, 0x336,8, 0x03, 0x01,0x05,0x03,0x03,0x00,0x00,0x00 );
t[ 4].set( 1000,225, 500, 0x324,8, 0x03, 0x01,0x02,0x00,0x00,0x00,0x00,0x00 );
t[ 5].set( 1000,250, 500, 0x337,8, 0x10, 0x2B, ' ', ' ', ' ', '@', ' ', ' ' );
t[ 6].set( 1000,275, 500, 0x337,8, 0x21,  ' ', 'M', 'e', 'r', 'c', '@', 'u' );
t[ 7].set( 1000,300, 500, 0x337,8, 0x22,  'r', 'y', ' ', ' ', ' ', ' ', ' ' );
t[ 8].set( 1000,325, 500, 0x337,8, 0x23,  ' ', ' ', ' ', ' ', ' ', '@', ' ' );
t[ 9].set( 1000,350, 500, 0x337,8, 0x24,  ' ', ' ', 'M', 'a', 'r', 'i', 'n' );
t[10].set( 1000,375, 500, 0x337,8, 0x25,  'e', 'r', ' ', ' ', ' ', ' ', ' ' );
t[11].set( 1000,400, 500, 0x337,8, 0x26,  ' ', ' ',0x00,0x00,0x00,0x00,0x00 );
}
```

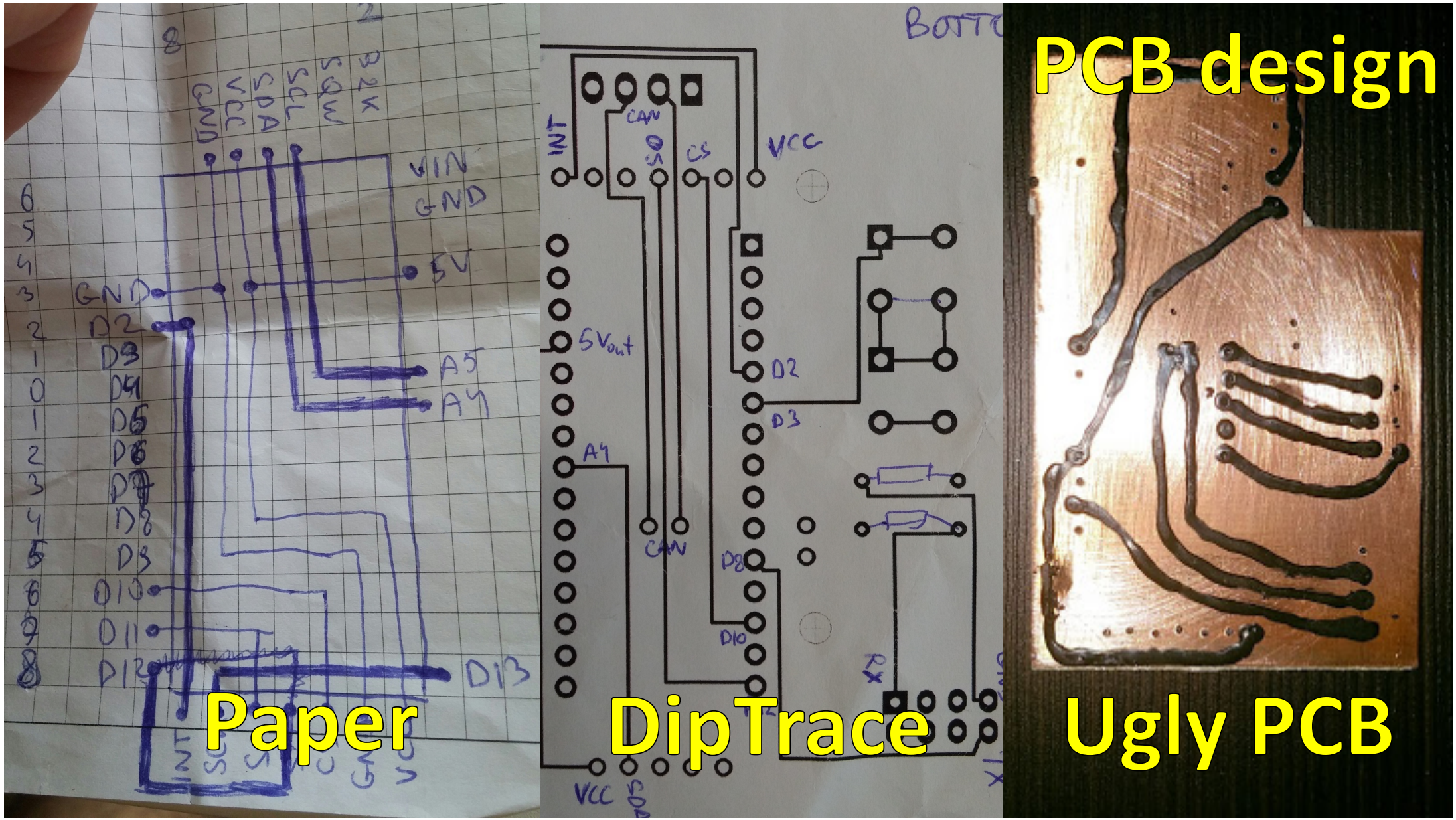
Each 50 ms

Full cycle 500 ms

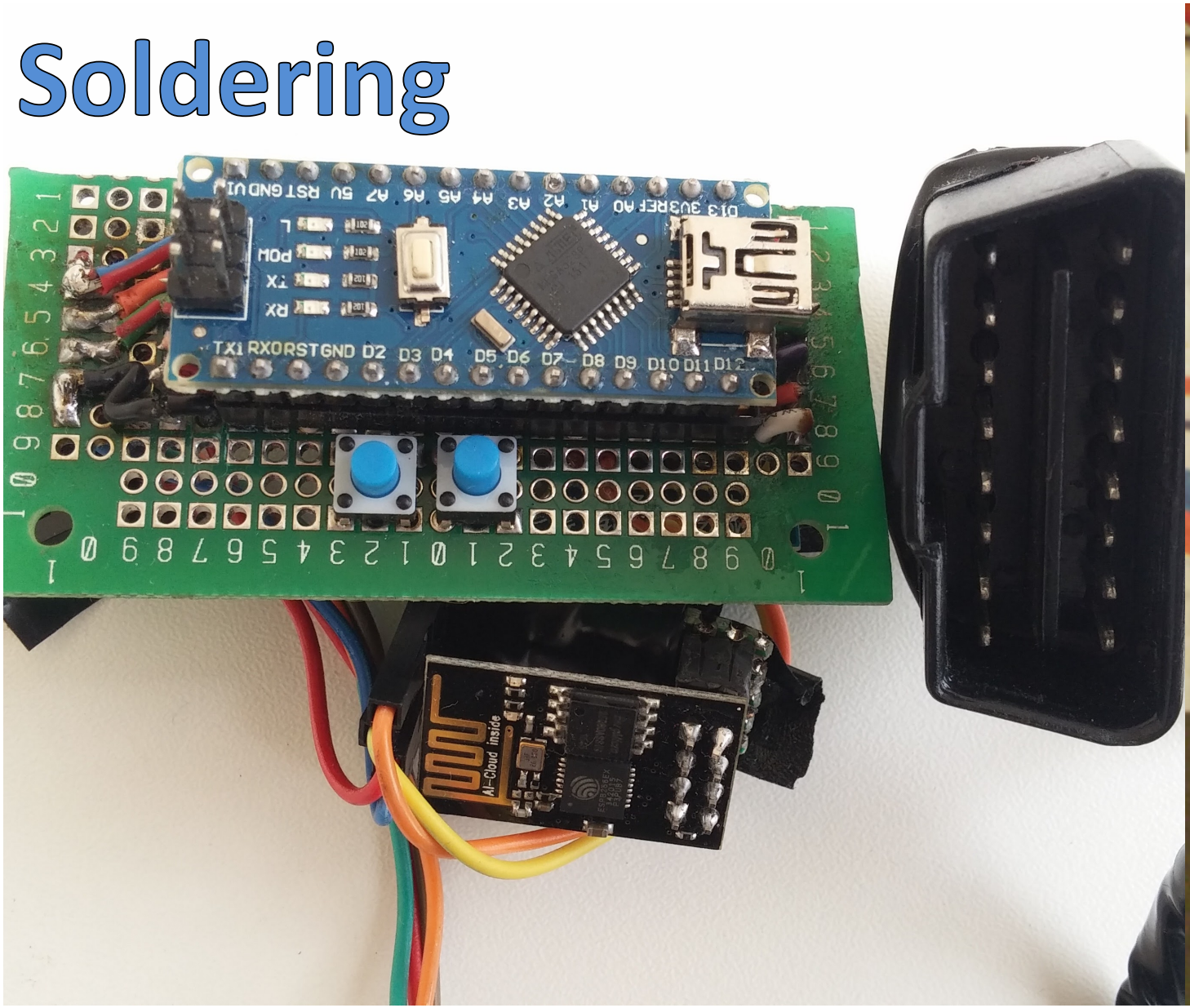
0x337 - characters
0x336, 0x324 - control

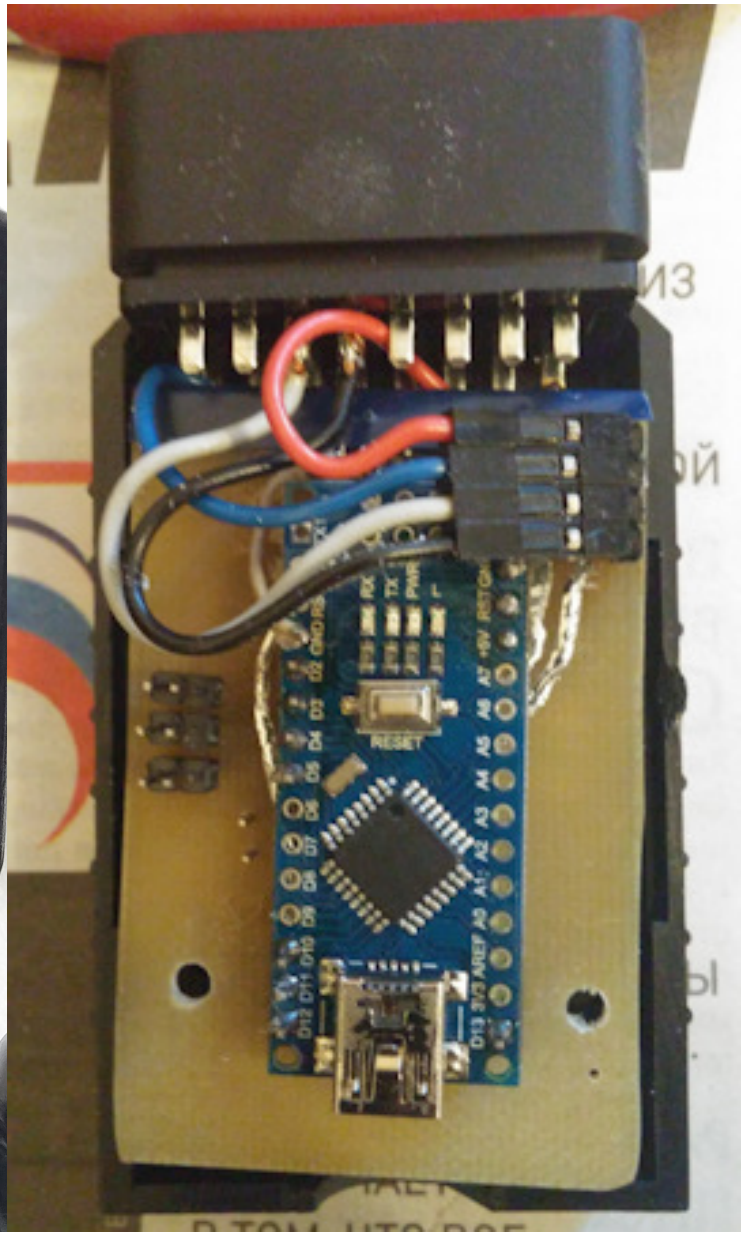
Receiving CAN messages

```
void MCP2515_ISR()
{
    rcvFlag = 1;
}
attachInterrupt(0, MCP2515_ISR, FALLING);

CAN.init_Mask(0, 0, 0x7FF << 18);
CAN.init_Mask(1, 0, 0x7FF << 18);
CAN.init_Filt(0, 0, 0x423 << 18);

...
  if (rcvFlag == 1) {
    rcvFlag = 0;
    while (CAN_MSGAVAIL == CAN.checkReceive()) {
      CAN.readMsgBuf(&rcvLen, rcvBuf);
      rcvCanId = CAN.getCanId();
      if (rcvCanId == 0x423)
          rpm = String(( ( rcvBuf[2] << 8 ) + rcvBuf[3] ) / 4);
      }
  }
...
```


PCB design
Paper
DipTrace
Ugly PCB
GND
VCC
SDA
SCL
SCK
MOSI
MISO
RST
VIN
GND
5V
A5
A4
D2
D3
D4
D5
D6
D7
D8
D9
D10
D11
D12
D13
INT
CAN
CS
5Vout
RX
TX

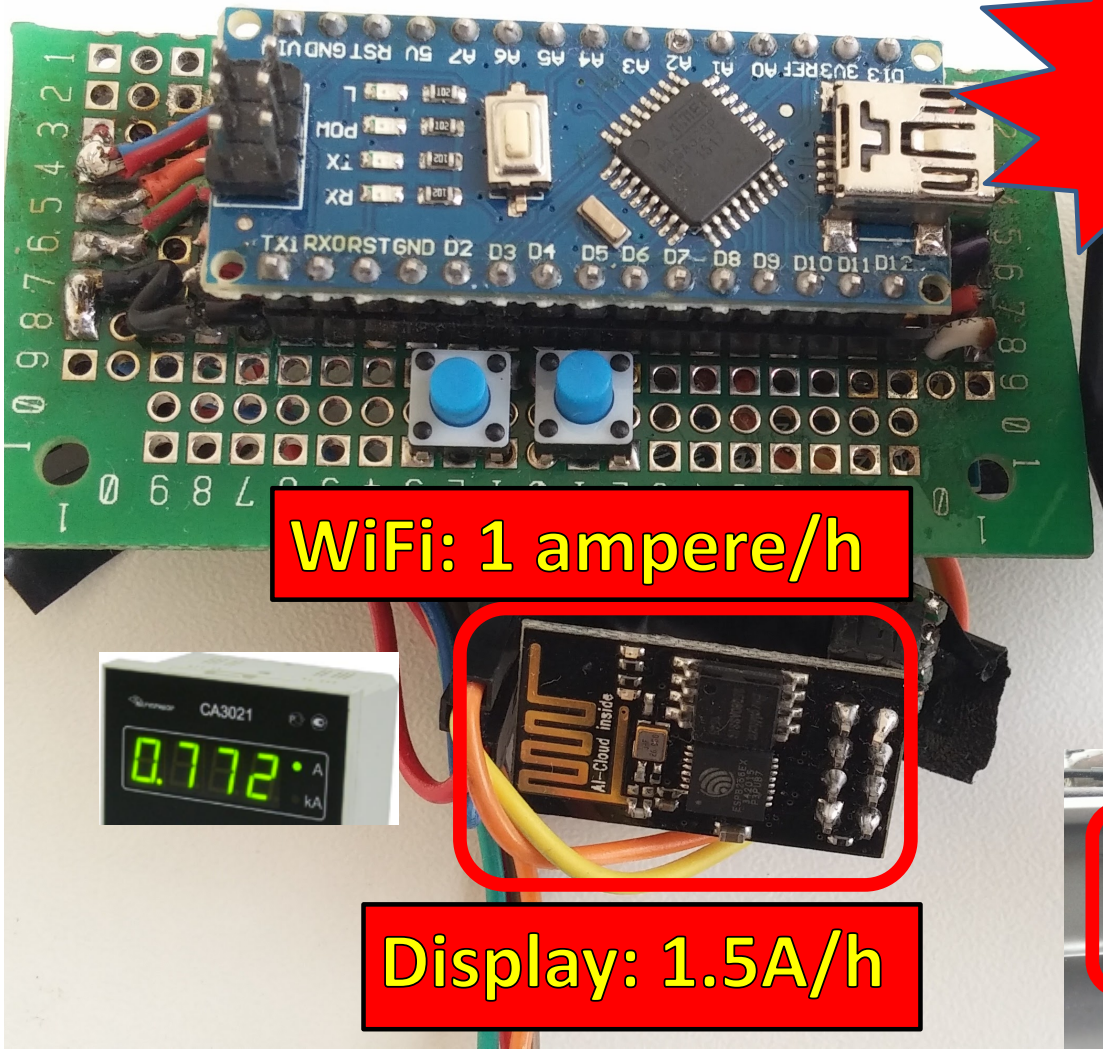
Soldering


TX1 RXO RST GND D2 D3 D4 D5 D6 D7 D8 D9 D10 D11 D12
AI-Cloud inside


RESET


0
MSI
32 We've got the 33
32 RPM: 756 T: 79 33
E
EXT TEMP
-9
Happiness
is almost here

Current draw!



Display: 1.5A/h

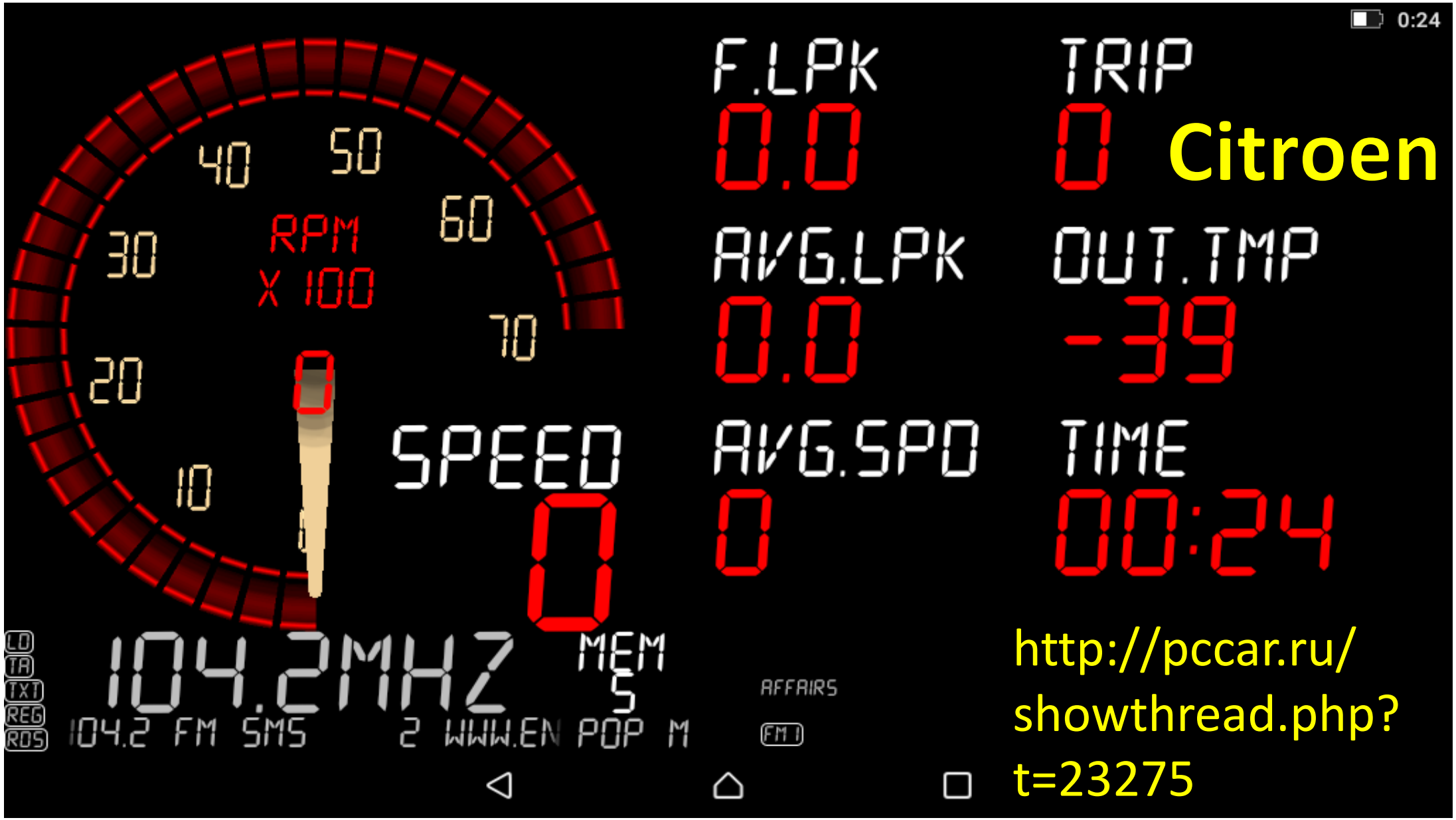
FAIL!

Other cars...

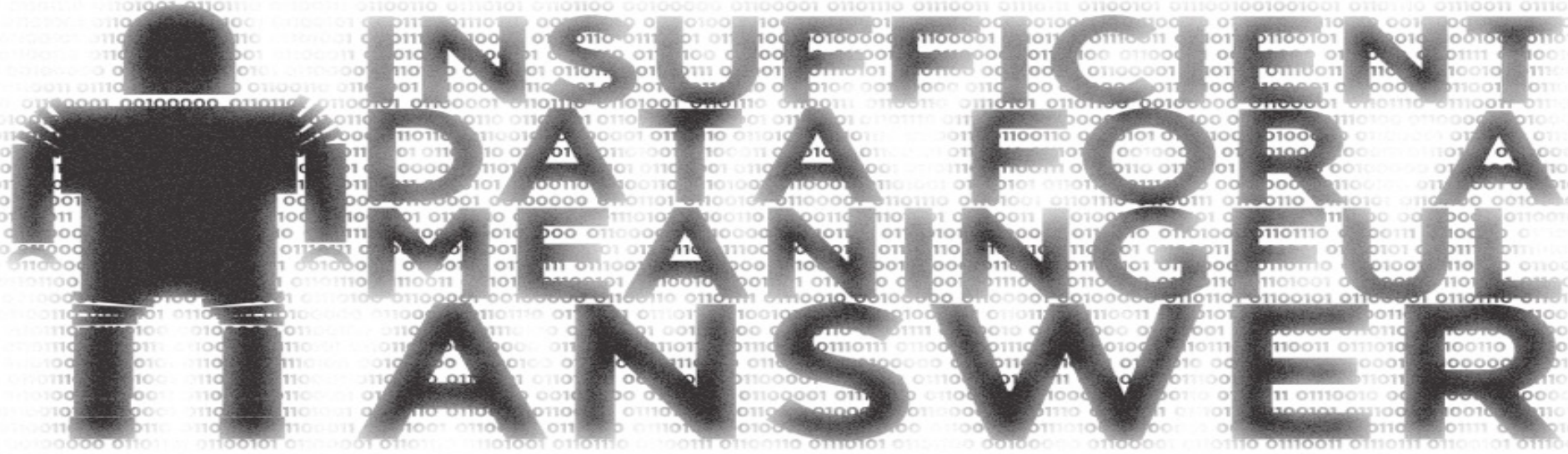

Jeep
20
140
160
100
E 51°F
Hacked!
http://chadgibbons.com/2013/12/29/hacking-the-jeep-interior-can-bus/


Mazda
x1000r/min
mph
TRIP A
RX-8 CAN control
www.cantanko.com
https://www.cantanko.com/rx-8/reverse-engineering-the-rx-8s-instrument-cluster-part-one/
http://www.madox.net/blog/projects/mazda-can-bus/


ANW 16:
ABTO
FM 1
km
73596 5
P R N D S
NAVIGATIO
N NE E
km
605 16
P R N D S
Volkswagen
http://pccar.ru/
showthread.php?
t=24102


0:24
F.LPK
0.0
TRIP
0
Citroen
AVG.LPK
0.0
OUT.TMP
-39
AVG.SPD
0
TIME
00:24
RPM
X 100
10
20
30
40
50
60
70
SPEED
0
104.2MHZ
MEM
5
LD
TA
TXT
REG
RDS
104.2 FM SMS
2 WWW.EN POP M
AFFAIRS
FM1
http://pccar.ru/showthread.php?t=23275

Questions? *



* I have lots myself…

nikita@nalyutin.com