Lightstone

We simplify the complex

~~From **Overheating** to **Overachieving**~~

Blowing **STUFF** Up!

trying

A ~~**Comedic**~~ **Tragic** Tale of **Hacking** My Car

…but still “useful”

^

~~@rudigrobler~~

anonymous

WHO AM I? (NOT)

Auto **Electrician**

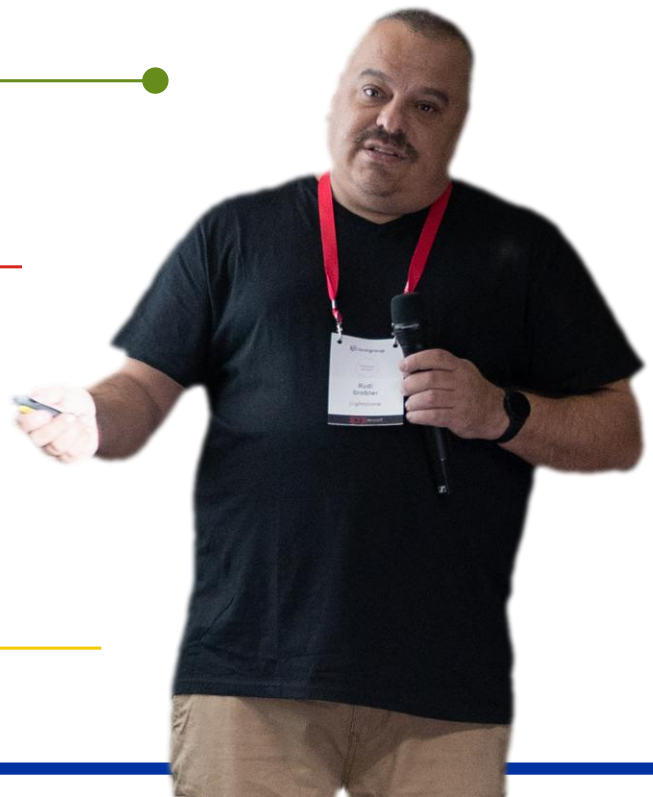
Mechanic

Developer @ Lightstone

We simplify the complex

Seasoned (synonym for old) software engineer who has been developing software for diverse vertical markets for over two decades.

@rudigrobler




SPACEX
“We’re going to make it happen.“
Elon Musk

THE PROBLEM

OLD CAR

Renault Kwid (2017)

OVERHEATING

The main, but not only problem was that it overheated!

REPAIR NOT EASY

Went to multiple repair shops, either thy returned it and said it had no problem, or “fixed” it and it still eventual gave the same issue…

THE PROBLEM

OLD CAR

Renault Kwid (2017)

OVERHEATING

The main, but not only problem was that it overheated!

REPAIR NOT EASY

Went to multiple repair shops, either thy returned it and said it had no problem, or “fixed” it and it still eventual gave the same issue…

THE PROBLEM

OLD CAR

Renault Kwid (2017)

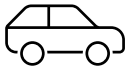
OVERHEATING

The main, but not only problem was that it overheated!

REPAIR NOT EASY

Went to multiple repair shops, either thy returned it and said it had no problem, or “fixed” it and it still eventual gave the same issue…

THE PLAN

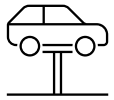


HACK THE CAR

Try to speak to the car…

ASK QUESTIONS

Like, what's your temperature?



SHOW IT SOMEWHERE

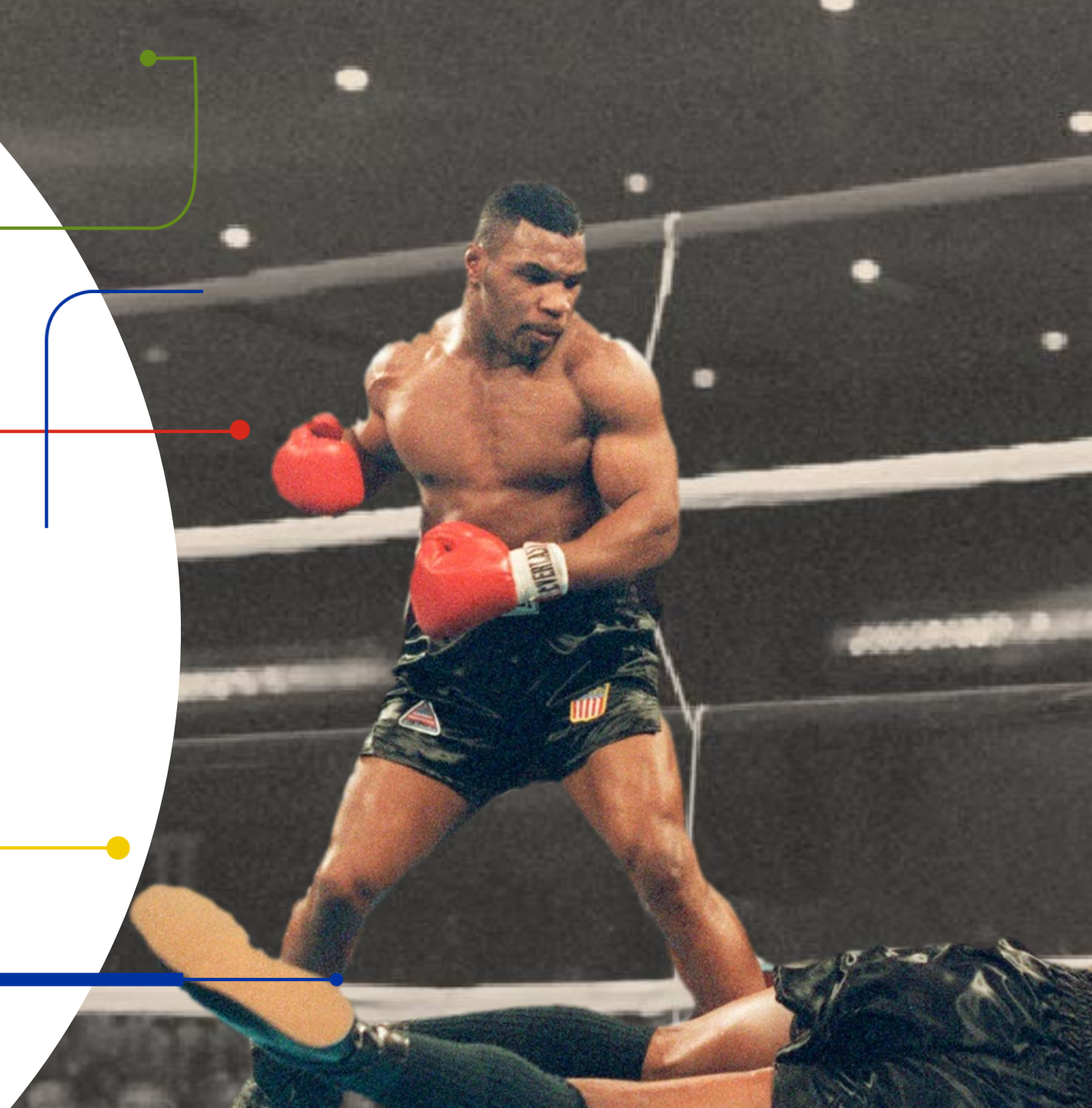
The dashboard sucked, but it has an 8” media screen, why not show stuff there?

“Like really… how **hard** can it be?”

@rudigrobler

“Everyone has a **plan**, until they get **punched** in the mouth”

Mike Tyson



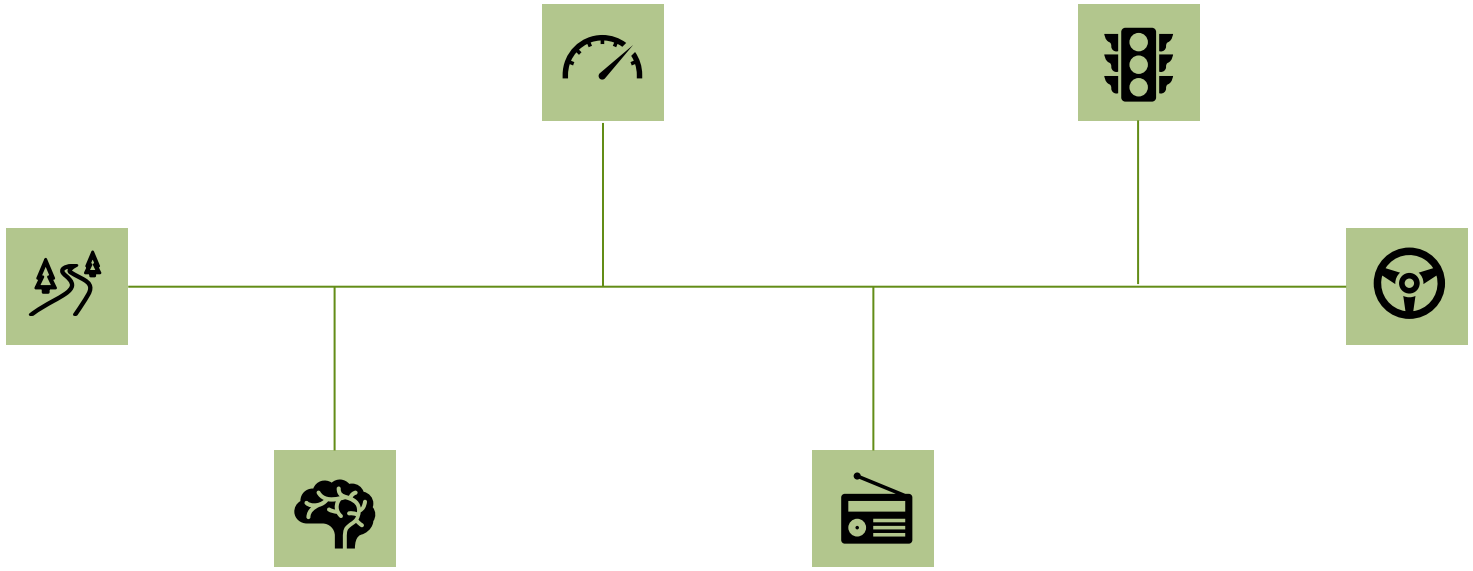
HOW?

There's an **EASY** way

and the **HARD** way….

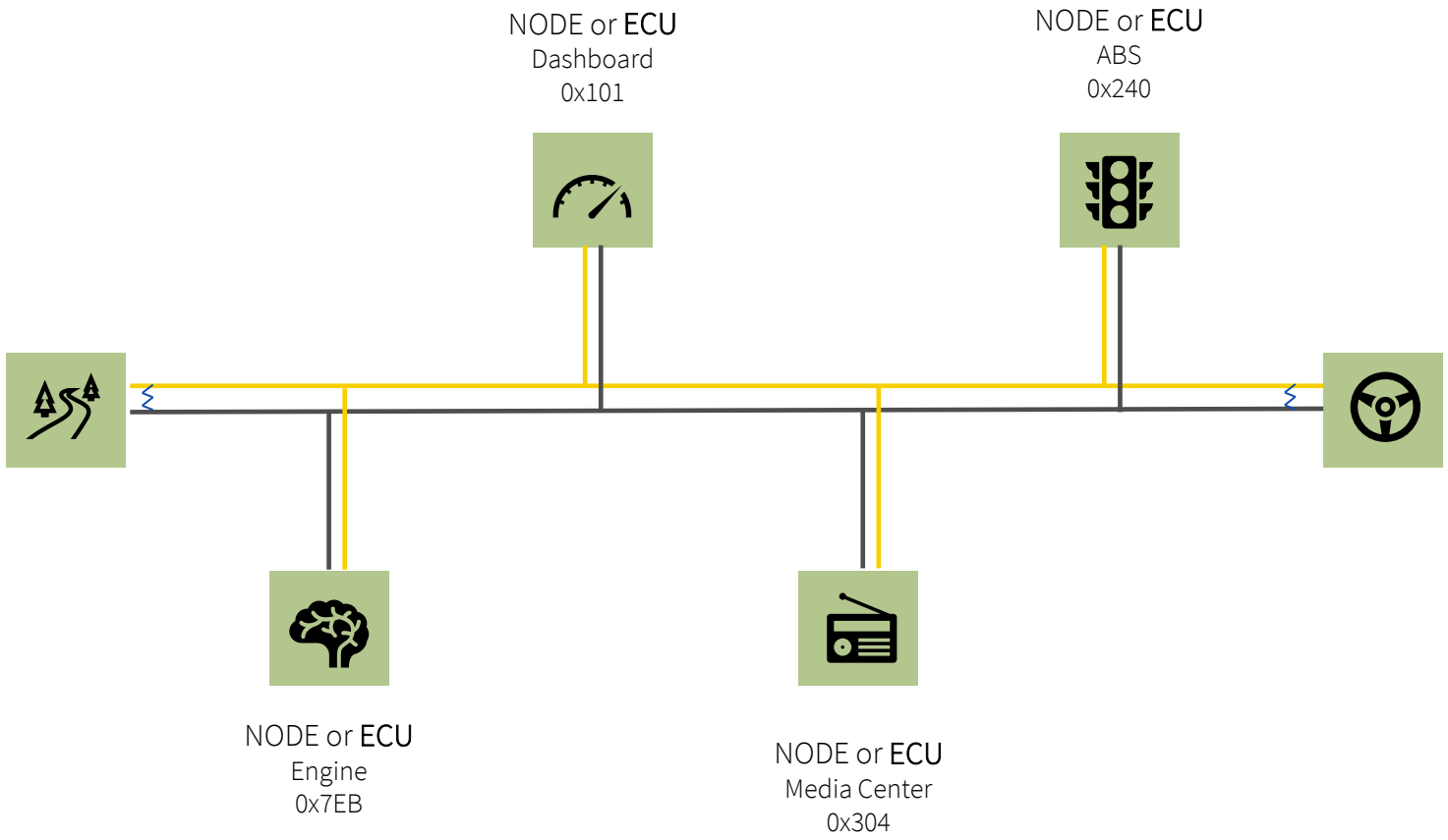
CARs

CAN



A Control Area Network (**CAN**) bus is a message-based protocol that allows devices to exchange data in a **reliable** and **efficient** way.

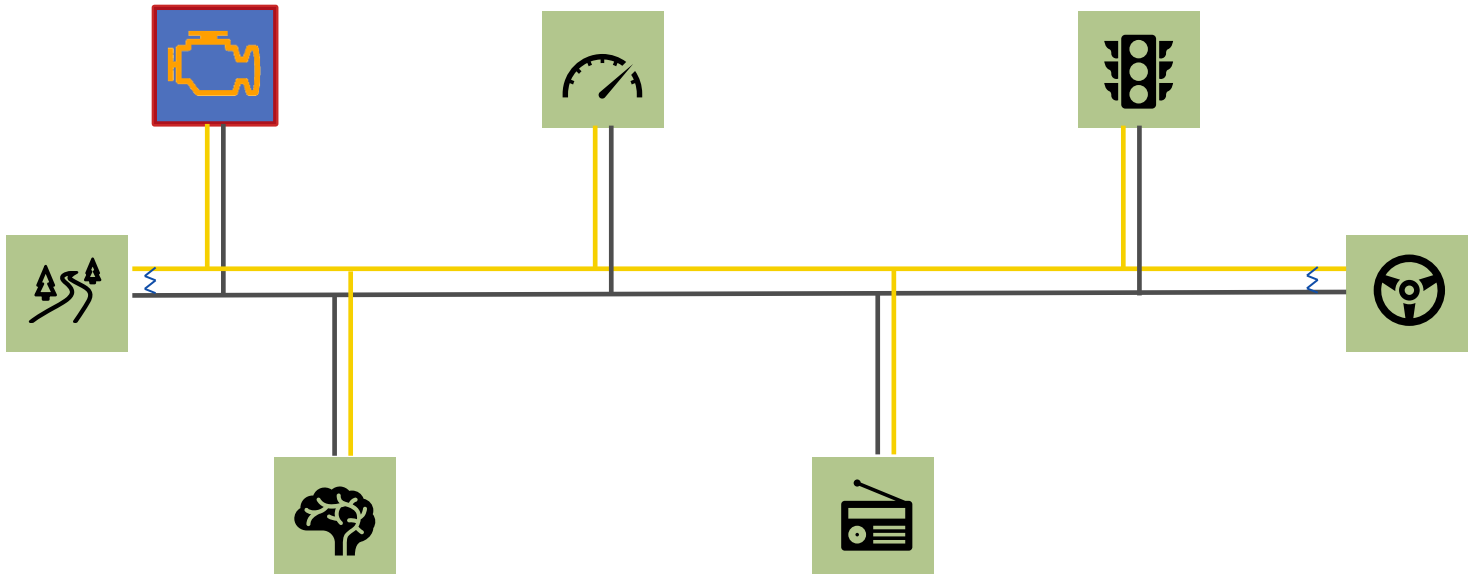
CAN


NODE or ECU
Dashboard
0x101
NODE or ECU
ABS
0x240
NODE or ECU
Engine
0x7EB
NODE or ECU
Media Center
0x304


CAN High
CAN Low

OBD

On board diagnostics (**OBD**) is a 'higher layer protocol' (like a **language**).



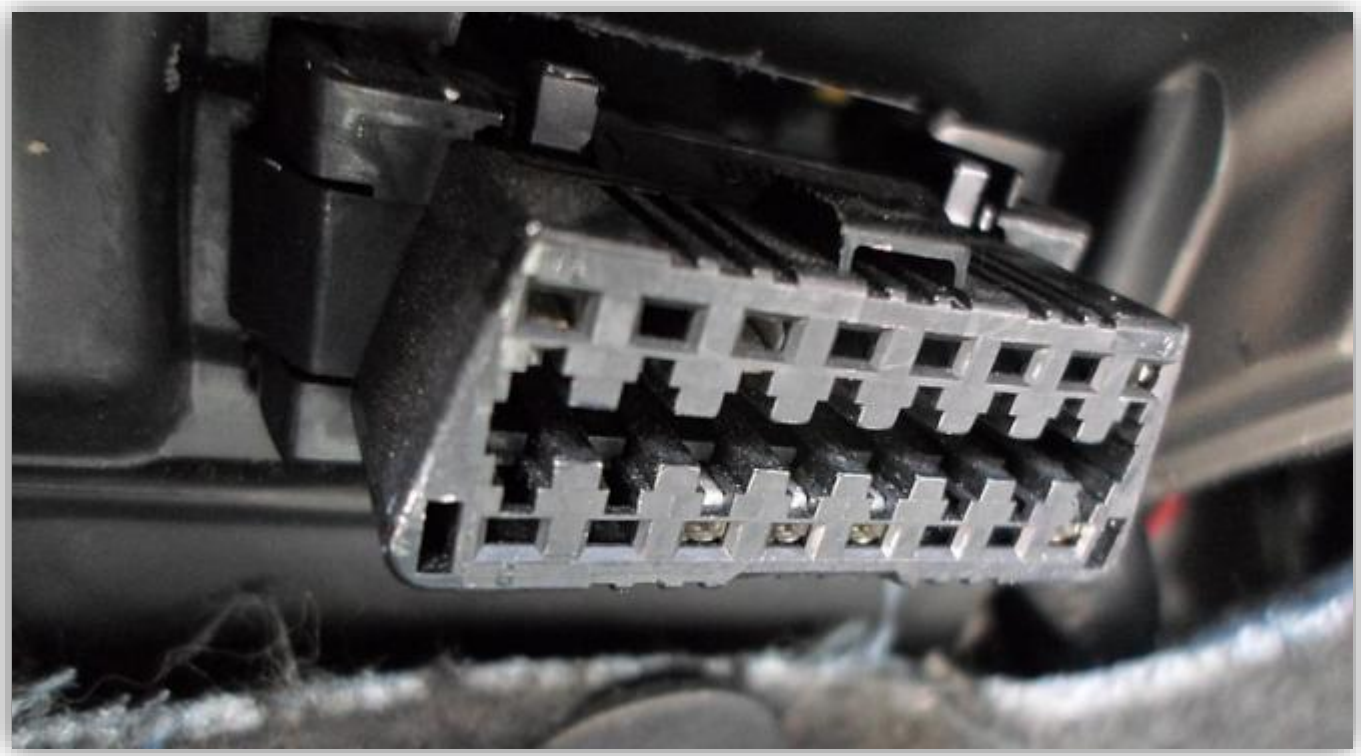
CAN is a **method** for communication (like a **phone**).

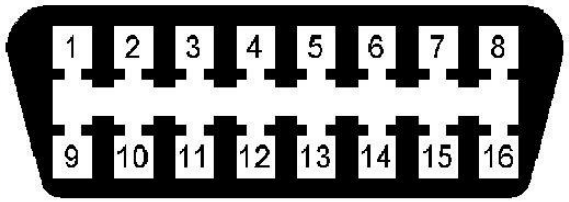
REQUIRED BY LAW

South Africa's carbon dioxide (CO_2) emissions tax for passenger cars.

Must be showed somewhere?

And must be measurable?





PIN	DESCRIPTION	PIN	DESCRIPTION
1	Vendor Option	9	Vendor Option
2	J1850 Bus +	10	j1850 BUS
3	Vendor Option	11	Vendor Option
4	Chassis Ground	12	Vendor Option
5	Signal Ground	13	Vendor Option
6	CAN (J-2234) High	14	CAN (J-2234) Low
7	ISO 9141-2 K-Line	15	ISO 9141-2 Low
8	Vendor Option	16	Battery Power

OBD-II Connector and Pinout

RENAULT

BMW

SUZUKI

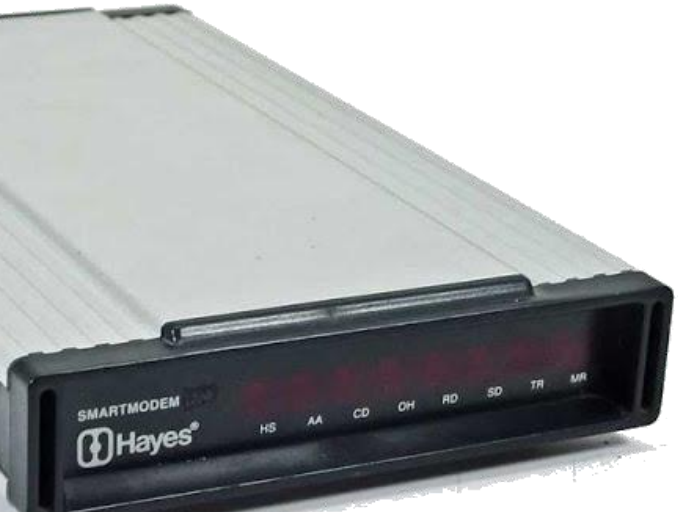
On Board Diagnostics

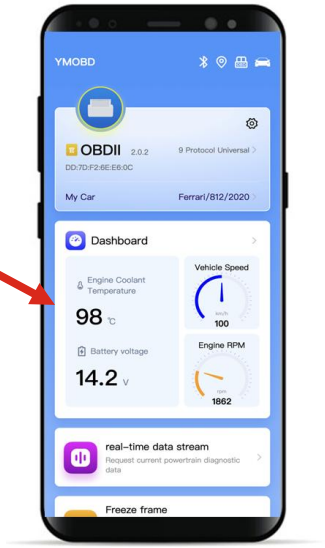
THE EASY WAY

Use an over-the-shelf OBD connector (like the **ELM327**)

It provide you with sensor data, like **TEMPERATURE**, speed and RPMs.

Simple **Bluetooth** adapter that can talk to your **phone**!

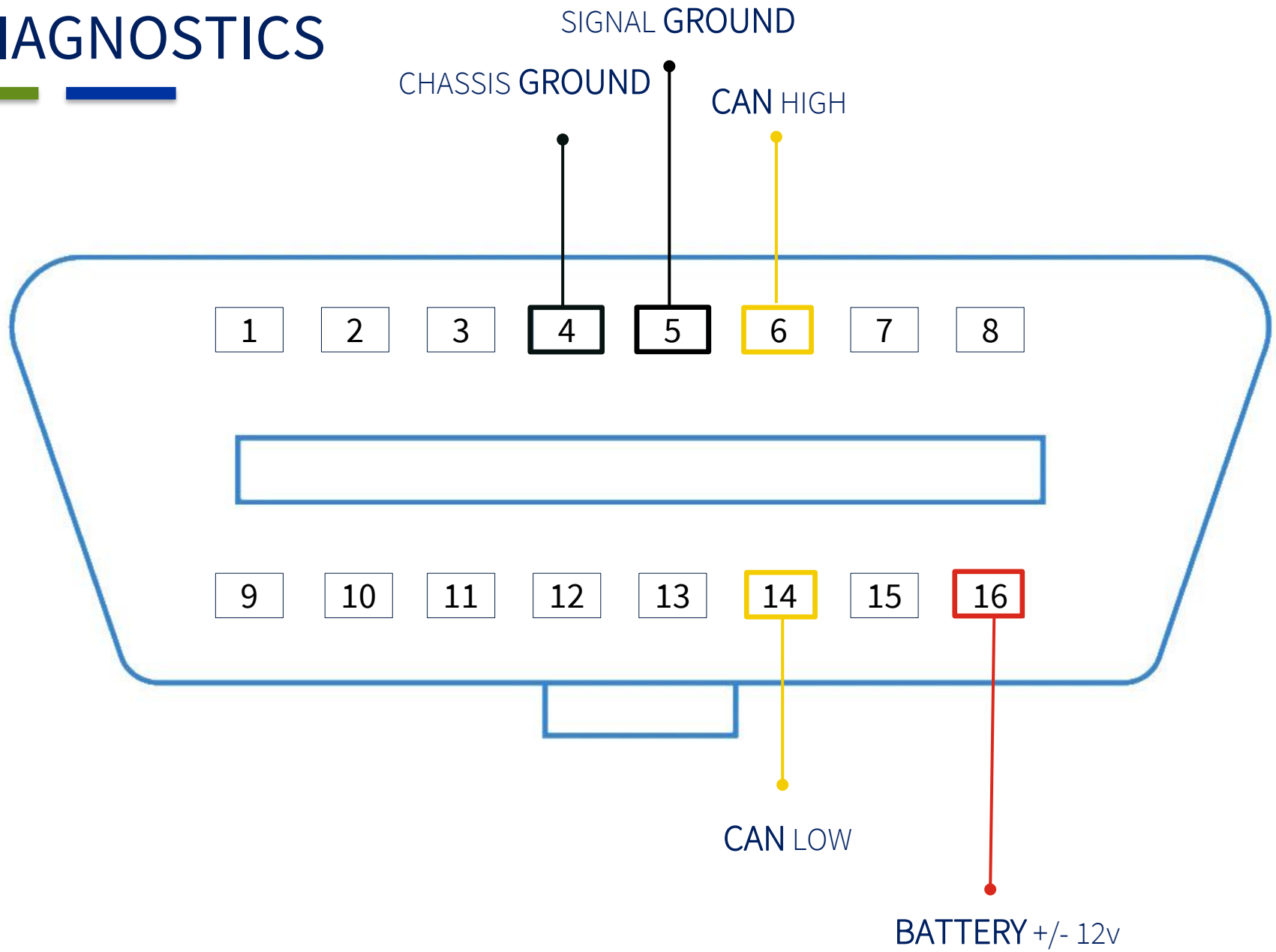


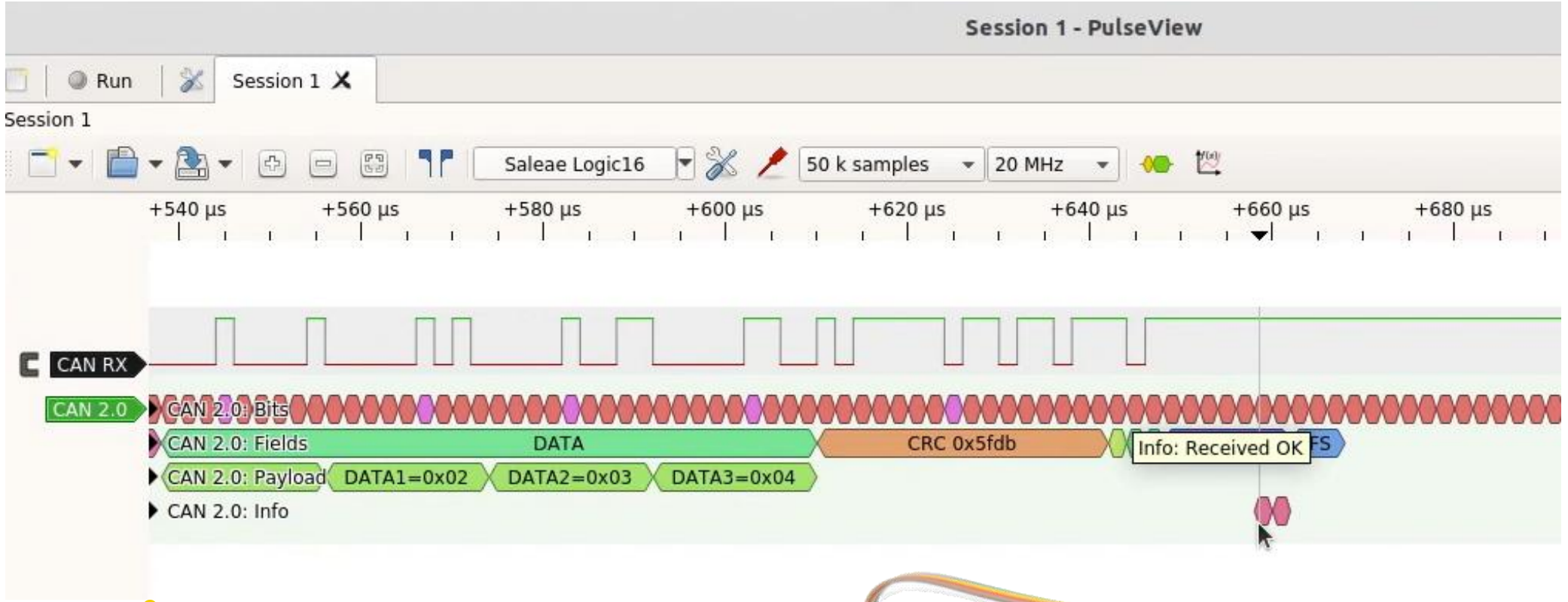


LIFE HAPPENS

Oops, I did it again…

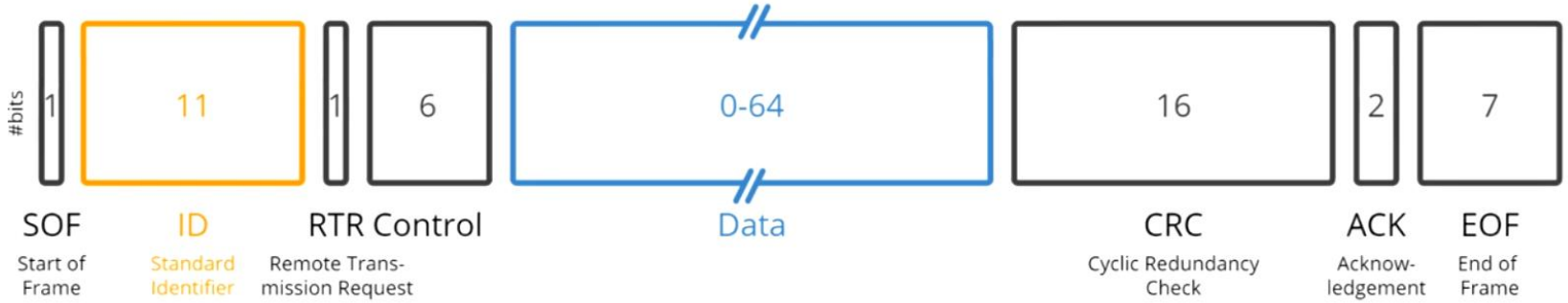
ON BOARD DIAGNOSTICS

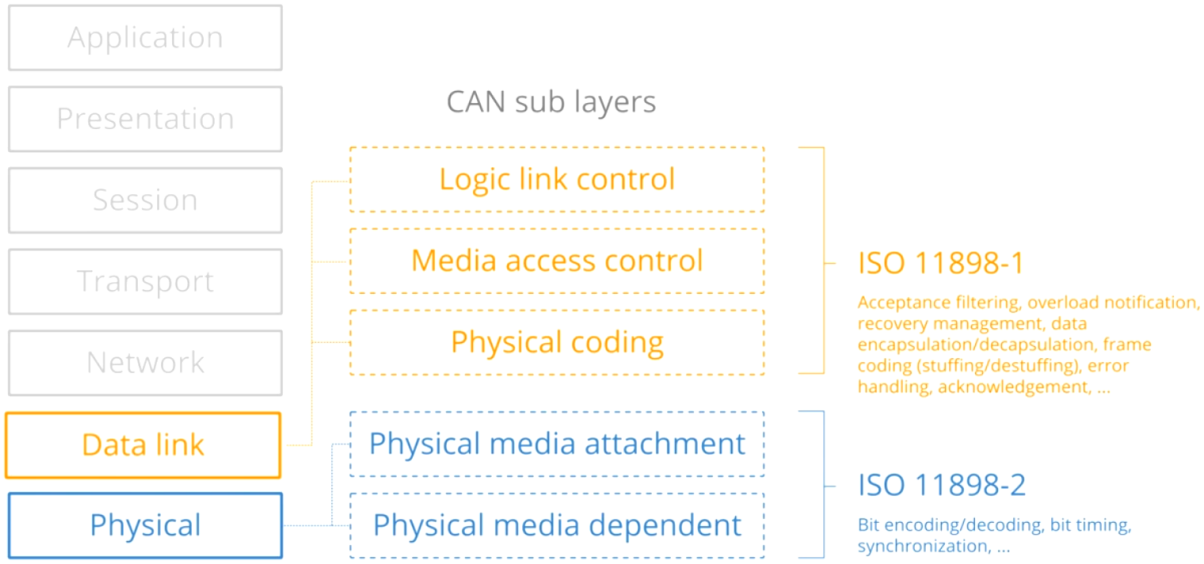



Session 1 - PulseView
Run
Session 1
Session 1
Saleae Logic16
50 k samples
20 MHz
+540 µs
+560 µs
+580 µs
+600 µs
+620 µs
+640 µs
+660 µs
+680 µs
CAN RX
CAN 2.0
CAN 2.0: Bits
CAN 2.0: Fields
DATA
CRC 0x5fdb
Info: Received OK
CAN 2.0: Payload
DATA1=0x02
DATA2=0x03
DATA3=0x04
CAN 2.0: Info


Logic
Analyzer
24MHz 8CH
CH1
CH3
CH5
CH7
CLK
CH2
CH4
CH6
CH8
GND

CAN

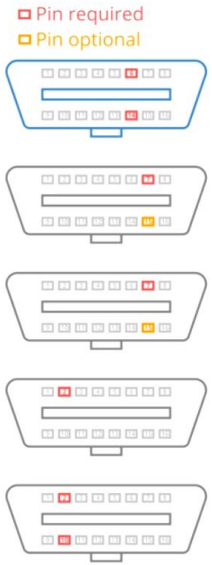

#bits
1
11
1
6
0-64
16
2
7
SOF
Start of Frame
ID
Standard Identifier
RTR Control
Remote Trans-mission Request
Data
CRC
Cyclic Redundancy Check
ACK
Acknow-ledgement
EOF
End of Frame


Application
Presentation
Session
Transport
Network
Data link
Physical
CAN sub layers
Logic link control
Media access control
Physical coding
Physical media attachment
Physical media dependent
ISO 11898-1
Acceptance filtering, overload notification, recovery management, data encapsulation/decapsulation, frame coding (stuffing/destuffing), error handling, acknowledgement, ...
ISO 11898-2
Bit encoding/decoding, bit timing, synchronization, ...

OBD via CAN

Identifier (e.g. 7E8)	#bytes (e.g. 03)	Mode (e.g. 41)	PID (e.g. 32)	A (e.g. AA)	B (e.g. AA)	B (e.g. AA)	D (e.g. AA)	E (e.g. AA)

ISO15765-4 (**CAN**)	Used in vast majority of cars today (mandatory since 2008)
ISO14230-4 (**KWP2000**)	Common protocol for 2003+ cars e.g. in Asia
ISO9141-2	Used mostly in EU, Chrysler & Asian cars in 2000-2004
SAE J1850 (**VPW**)	Used mostly in older GM cars
SAE J1850 (**PWM**)	Used mostly in older Ford cars



WIKIPEDIA
The Free Encyclopedia

Services / Modes [edit]

There are 10 diagnostic services described in the latest OBD-II standard SAE J1979. Before 2002, J1979 referred to these services as are as follows:

Service / Mode (hex)	Description
01	Show current data
02	Show freeze frame data
03	Show stored Diagnostic Trouble Codes
04	Clear Diagnostic Trouble Codes and stored values
05	Test results, oxygen sensor monitoring (non CAN only)
06	Test results, other component/system monitoring (Test results, oxygen sensor monitoring for CAN only)
07	Show pending Diagnostic Trouble Codes (detected during current or last driving cycle)
08	Control operation of on-board component/system
09	Request vehicle information
0A	Permanent Diagnostic Trouble Codes (DTCs) (Cleared DTCs)

Vehicle manufacturers are not required to support all services. Each manufacturer may define additional services above #9 (e.g.: servic

Modes

https://en.wikipedia.org/wiki/OBD-II_PIDs

WIKIPEDIA
The Free Encyclopedia

PIDs

06	6	1	Bank 1	-100 (Reduce Fuel: Too Rich)	99.2 (Add Fuel: Too Lean)	%	$\frac{100}{128}A - 100$ (or $\frac{A}{1.28} - 100$)
07	7	1	Long term fuel trim (LTFT)—Bank 1				
08	8	1	Short term fuel trim (STFT)—Bank 2				
09	9	1	Long term fuel trim (LTFT)—Bank 2				
0A	10	1	Fuel pressure (gauge pressure)	0	765	kPa	$3A$
0B	11	1	Intake manifold absolute pressure	0	255	kPa	A
0C	12	2	Engine speed	0	16,383.75	rpm	$\frac{256A + B}{4}$
0D	13	1	Vehicle speed	0	255	km/h	A
0E	14	1	Timing advance	-64	63.5	° before TDC	$\frac{A}{2} - 64$
0F	15	1	Intake air temperature	-40	215	°C	$A - 40$
10	16	2	Mass air flow sensor (MAF) air flow rate	0	655.35	g/s	$\frac{256A + B}{100}$
11	17	1	Throttle position	0	100	%	$\frac{100}{255}A$
12	18	1	Commanded secondary air status				Bit encoded. See below
13	19	1	Oxygen sensors present (in 2 banks)				[A0..A3] == Bank 1, Sensors 1-4. [A4..A7] == Bank 2...

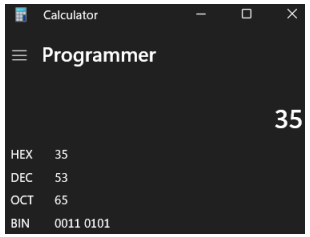
https://en.wikipedia.org/wiki/OBD-II_PIDs

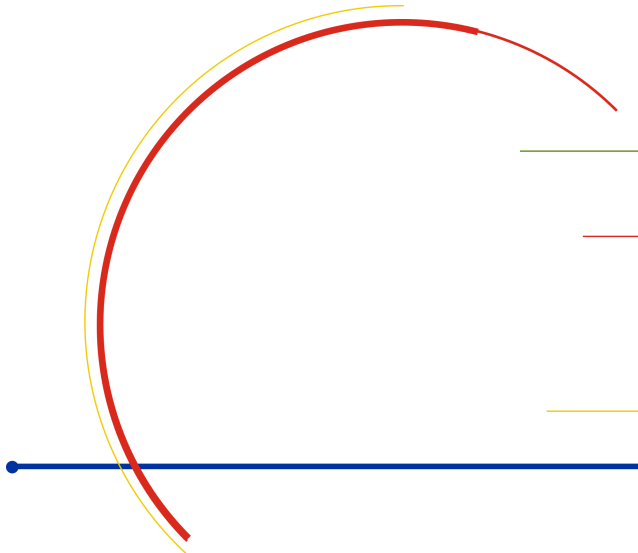
Identifier	#bytes	Mode	PID	A	B	B	D	E
7DF	02	01	0D	55	55	55	55	55
7E8	03	41	0D	35	AA	AA	AA	AA

53 Km/h

PID 0x0D

Vehicle speed





sketch_feb19a | Arduino IDE 2.3.1

File Edit Sketch Tools Help

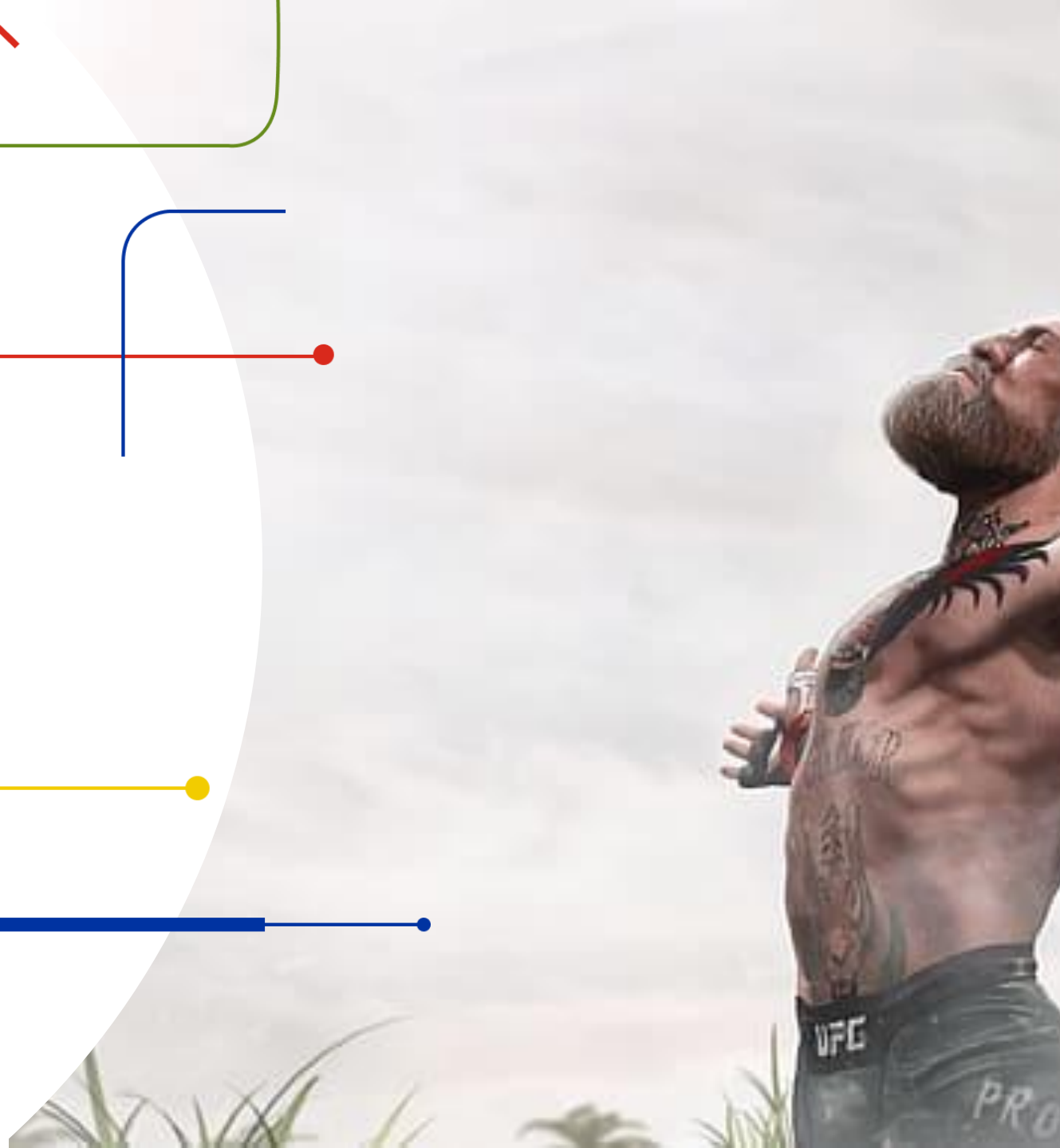
Select Board

sketch_feb19a.ino

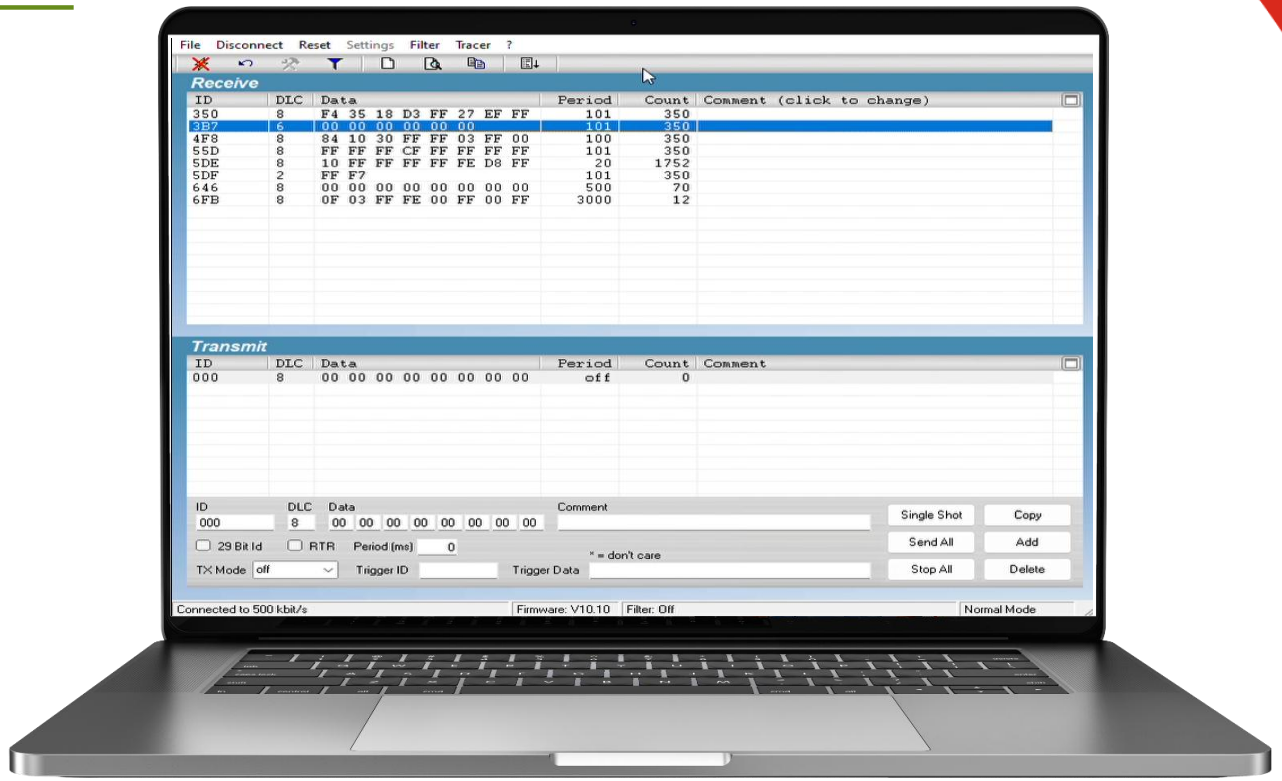
```
#include <SPI.h>
#include "mcp_can.h"

const int SPI_CS_PIN = 9;
MCP_CAN CAN0(SPI_CS_PIN);

#define PID_VEHICLE_SPEED   0x0D
#define CAN_ID_PID          0x7DF

void setup(){
  CAN0.begin(MCP_STD, CAN_500KBPS, MCP_8MHZ);
  CAN0.setMode(MCP_NORMAL);
}

void sendPid(unsigned char __pid)
{
  unsigned char tmp[8] = {0x02, 0x01, __pid, 0x55, 0x55, 0x55, 0x55, 0x55};
  CAN0.sendMsgBuf(CAN_ID_PID, 0, 8, tmp);
}

void loop() {
  // TODO
}
```

“There are **levels** to this game”

Conor McGregor



THE HARD WAY

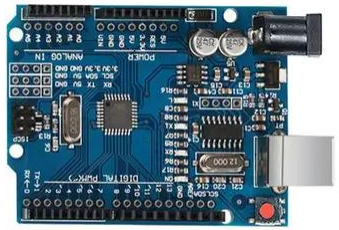


CANHacker is a software that can send and receive **CAN-Bus** messages.

SavvyCAN

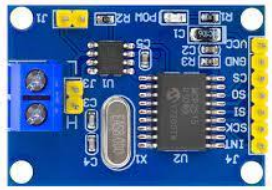
PEAK System

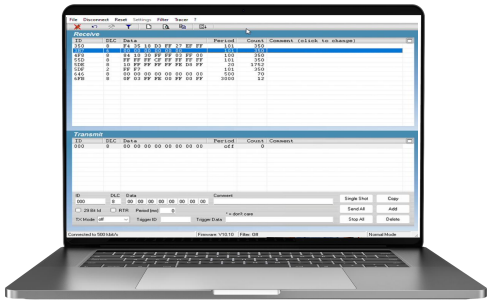
comma.ai



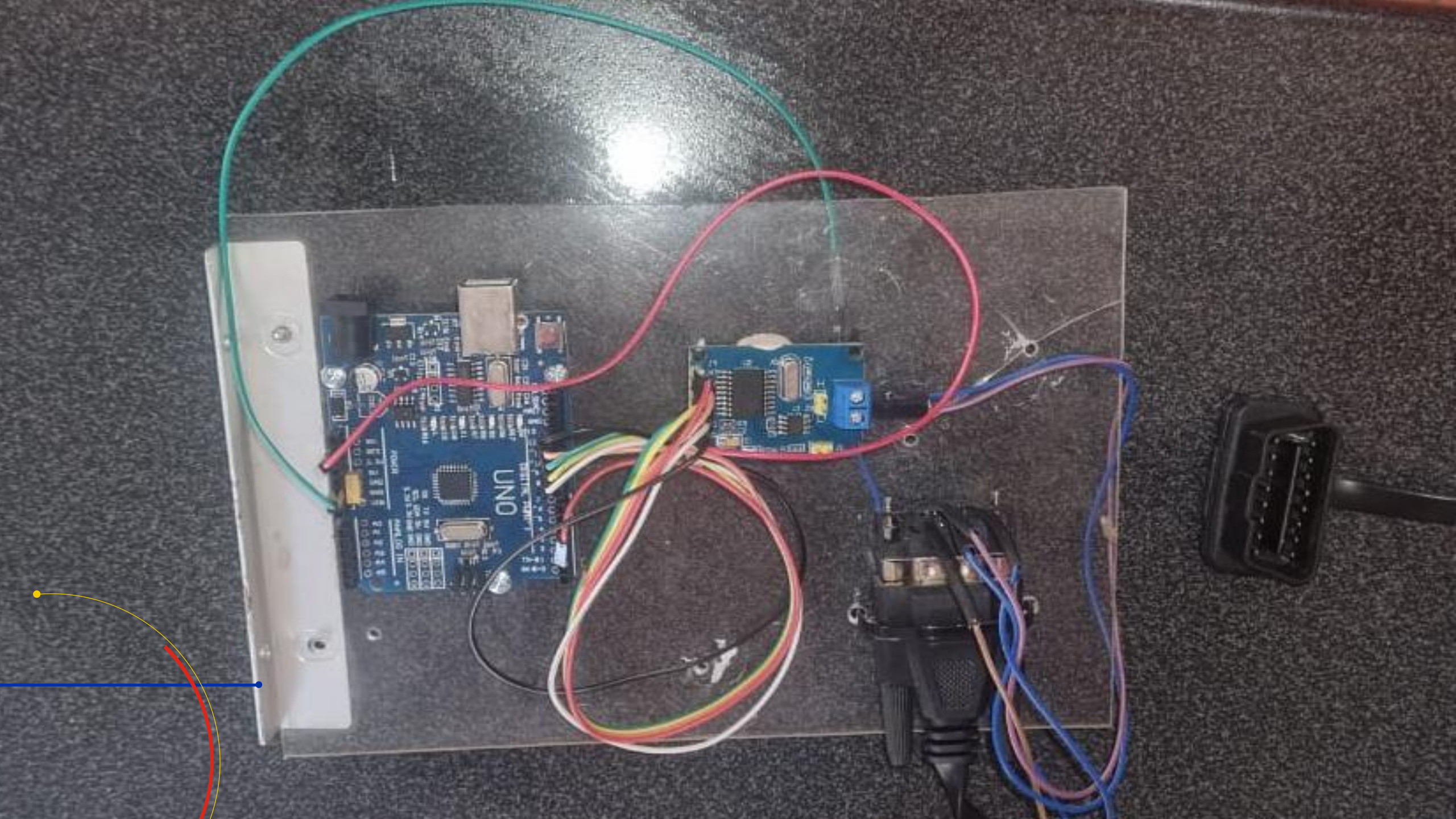
MCP2515

Arduino Uno
RP2040

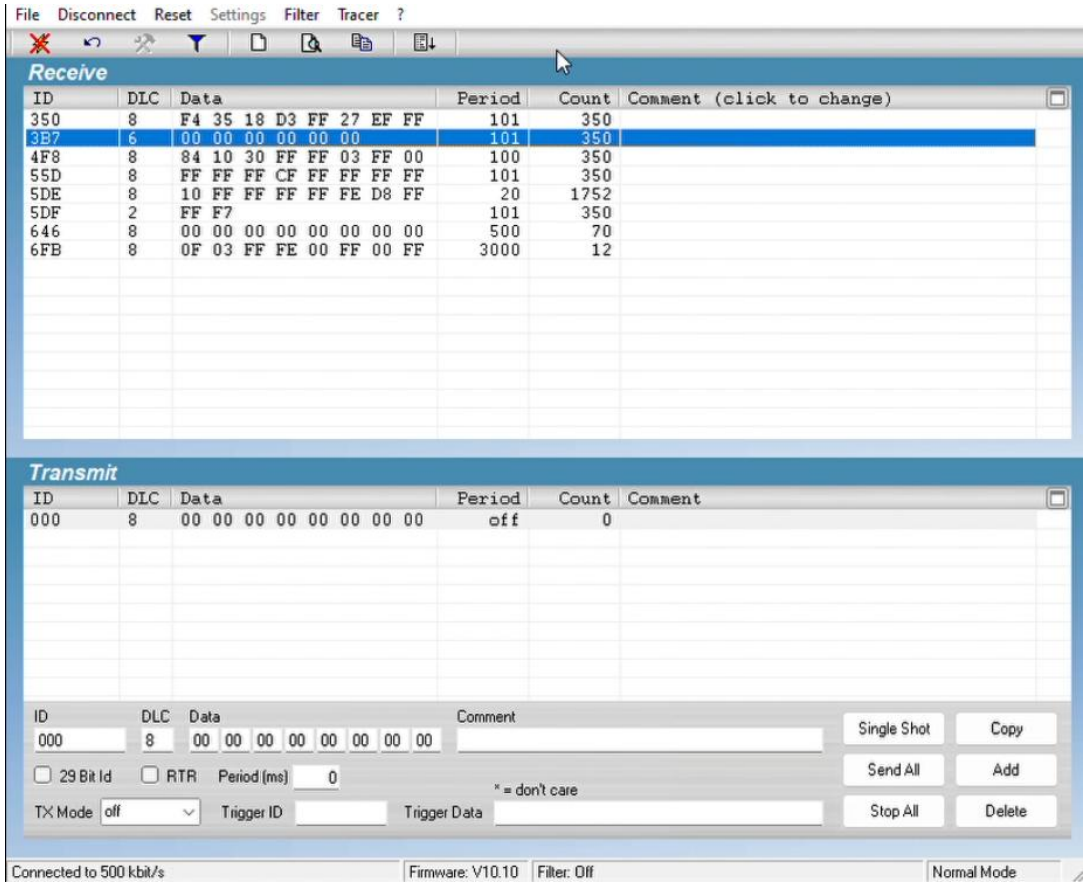




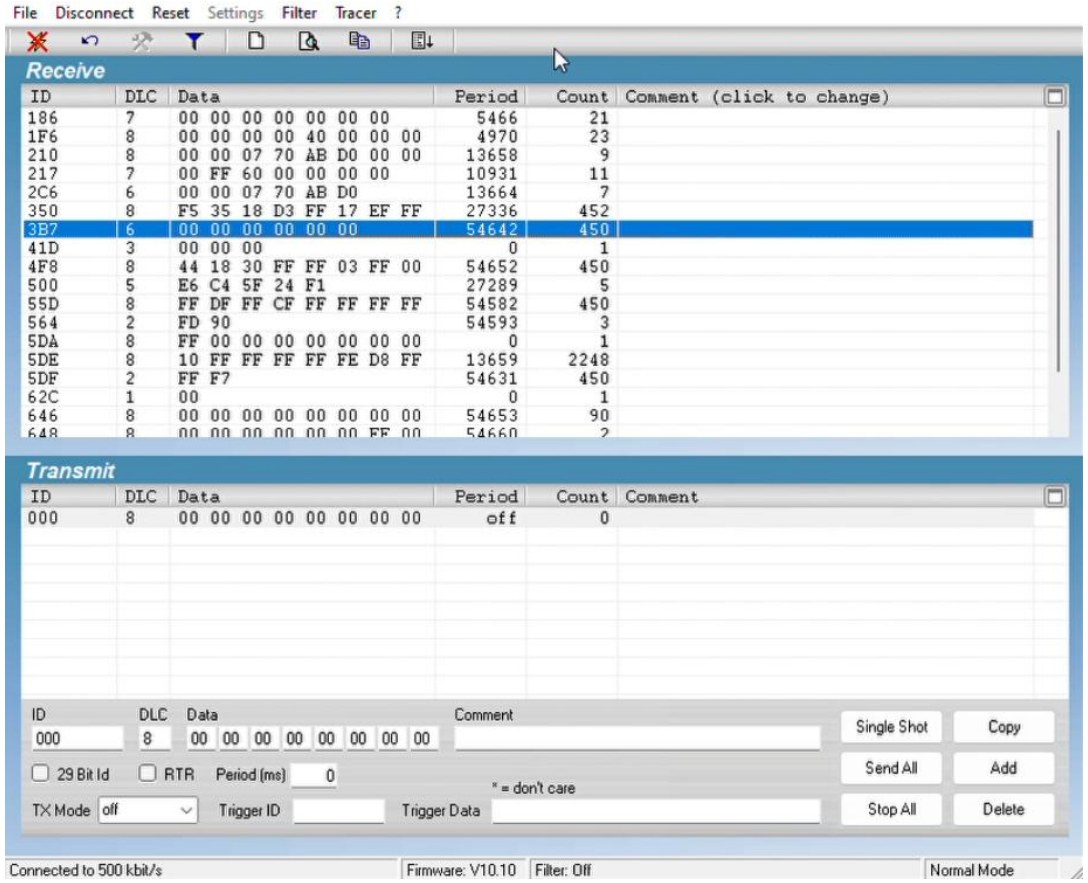
https://github.com/omarKmekkawy/**Arduino_CANHacker**


UNO

CAN – CAR OFF


File Disconnect Reset Settings Filter Tracer ?
Receive
ID DLC Data Period Count Comment (click to change)
350 8 F4 35 18 D3 FF 27 EF FF 101 350
3B7 6 00 00 00 00 00 00 101 350
4F8 8 84 10 30 FF FF 03 FF 00 100 350
55D 8 FF FF FF CF FF FF FF FF 101 350
5DE 8 10 FF FF FF FF FE D8 FF 20 1752
5DF 2 FF F7 101 350
646 8 00 00 00 00 00 00 00 00 500 70
6FB 8 0F 03 FF FE 00 FF 00 FF 3000 12
Transmit
ID DLC Data Period Count Comment
000 8 00 00 00 00 00 00 00 00 off 0
ID DLC Data Comment
000 8 00 00 00 00 00 00 00 00
Single Shot
Copy
29 Bit Id
RTR
Period (ms) 0
Send All
Add
* = don't care
TX Mode off
Trigger ID
Trigger Data
Stop All
Delete
Connected to 500 kbit/s
Firmware: V10.10
Filter: Off
Normal Mode

CAN – CAR ON

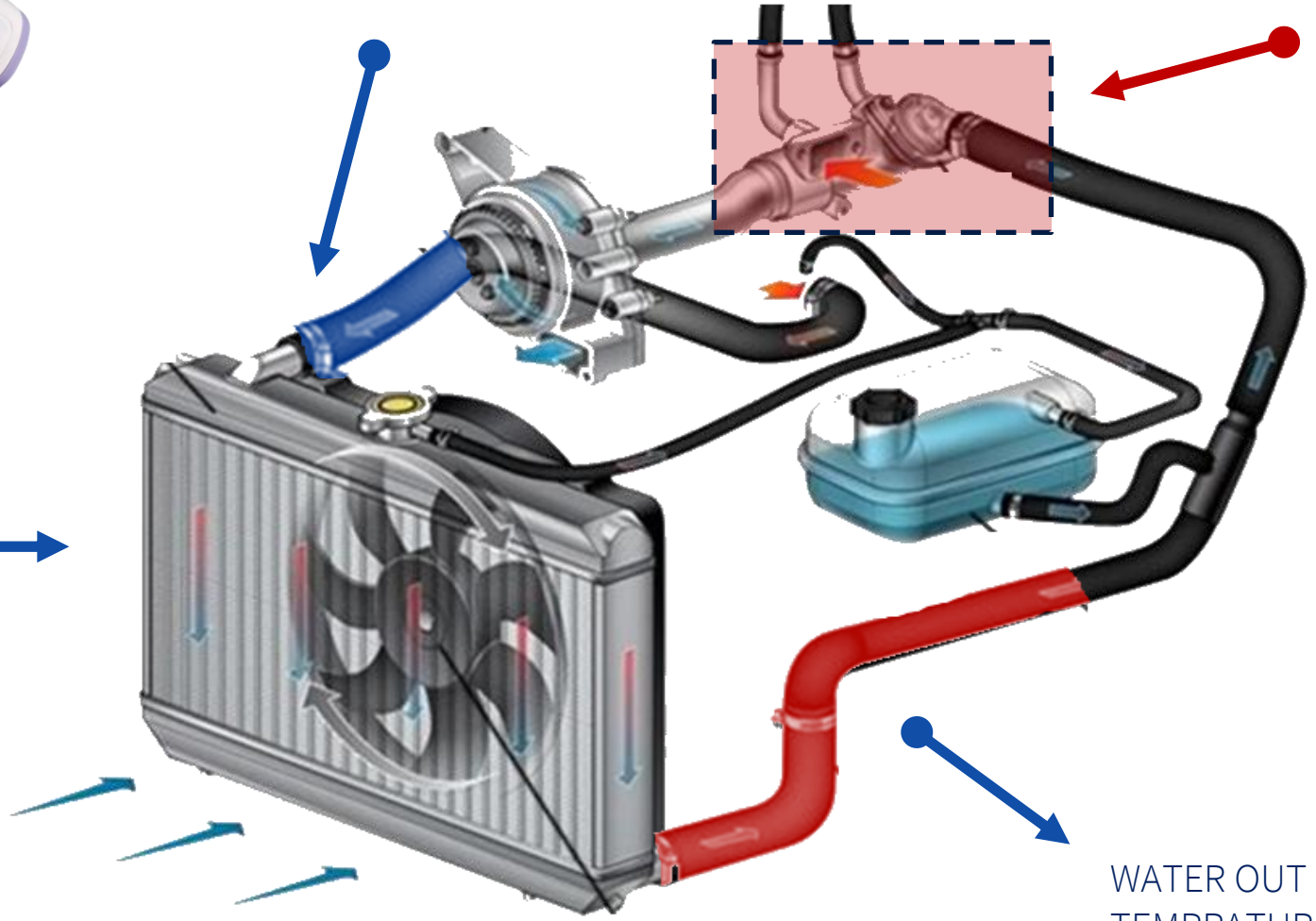

File Disconnect Reset Settings Filter Tracer ?
Receive
ID DLC Data Period Count Comment (click to change)
186 7 00 00 00 00 00 00 00 5466 21
1F6 8 00 00 00 00 40 00 00 00 4970 23
210 8 00 00 07 70 AB D0 00 00 13658 9
217 7 00 FF 60 00 00 00 00 10931 11
2C6 6 00 00 07 70 AB D0 13664 7
350 8 F5 35 18 D3 FF 17 EF FF 27336 452
3B7 6 00 00 00 00 00 00 54642 450
41D 3 00 00 00 0 1
4F8 8 44 18 30 FF FF 03 FF 00 54652 450
500 5 E6 C4 5F 24 F1 27289 5
55D 8 FF DF FF CF FF FF FF FF 54582 450
564 2 FD 90 54593 3
5DA 8 FF 00 00 00 00 00 00 00 0 1
5DE 8 10 FF FF FF FF FE D8 FF 13659 2248
5DF 2 FF F7 54631 450
62C 1 00 0 1
646 8 00 00 00 00 00 00 00 00 54653 90
Transmit
ID DLC Data Period Count Comment
000 8 00 00 00 00 00 00 00 00 off 0
ID DLC Data Comment
000 8 00 00 00 00 00 00 00 00
Single Shot
Copy
29 Bit Id
RTR
Period (ms) 0
Send All
Add
* = don't care
TX Mode off
Trigger ID
Trigger Data
Stop All
Delete
Connected to 500 kbit/s
Firmware: V10.10
Filter: Off
Normal Mode

“Everyone **lies.**”

House (MD)

WATER IN
TEMPRATURE

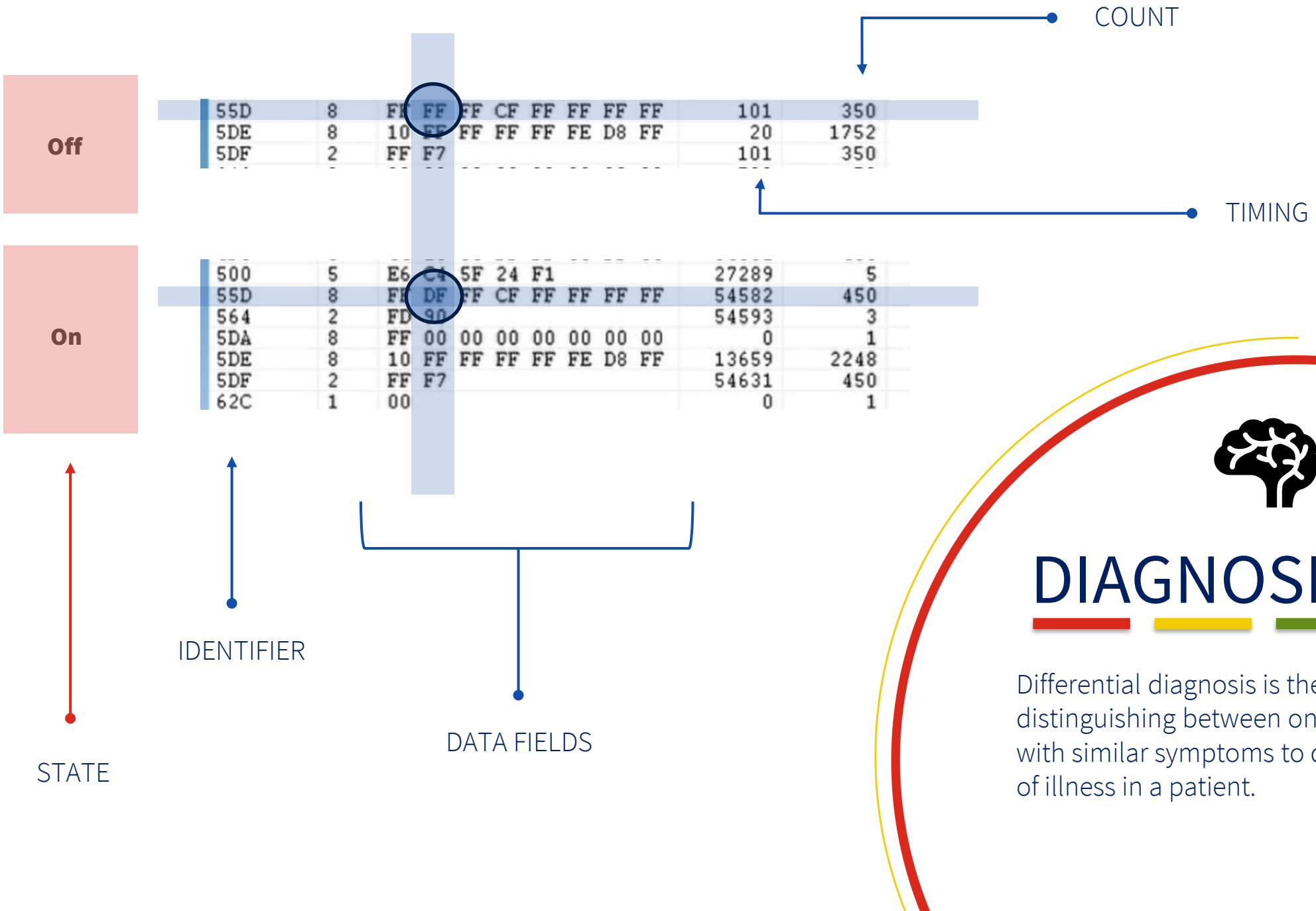
THERMOSTAT



COOLENT
TEMPRATURE

WATER OUT
TEMPRATURE

WATER OUT TEMP – WATER IN TEMP vs COOLENT TEMP



DIAGNOSIS

Differential diagnosis is the process of distinguishing between one disease and others with similar symptoms to determine the cause of illness in a patient.

WHY?

What can go

wrong?

WHY NOT?

Reduce total km driven

Intercept messages between ECU and dash?

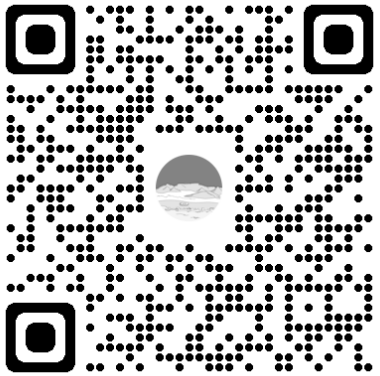
```
while (1) {
  send_message_with_id_0()
}
```

DoS Attack

Hardware Arbitration + Trusted Network

"The **harder** I practice, the **luckier** I got."

Gary Player



Lightstone

We simplify the complex

Thank You

@rudigrobler