
PATEL FOODS
INDO / PAK
HALAL MART
SICHUAN DYNASTY
BLUSH FITNESS
FITNESS DESIGNED FOR WOMEN
KOSHER FOODS
7206
KANSAS
HAKCER
mazda
Missouri
SECKC

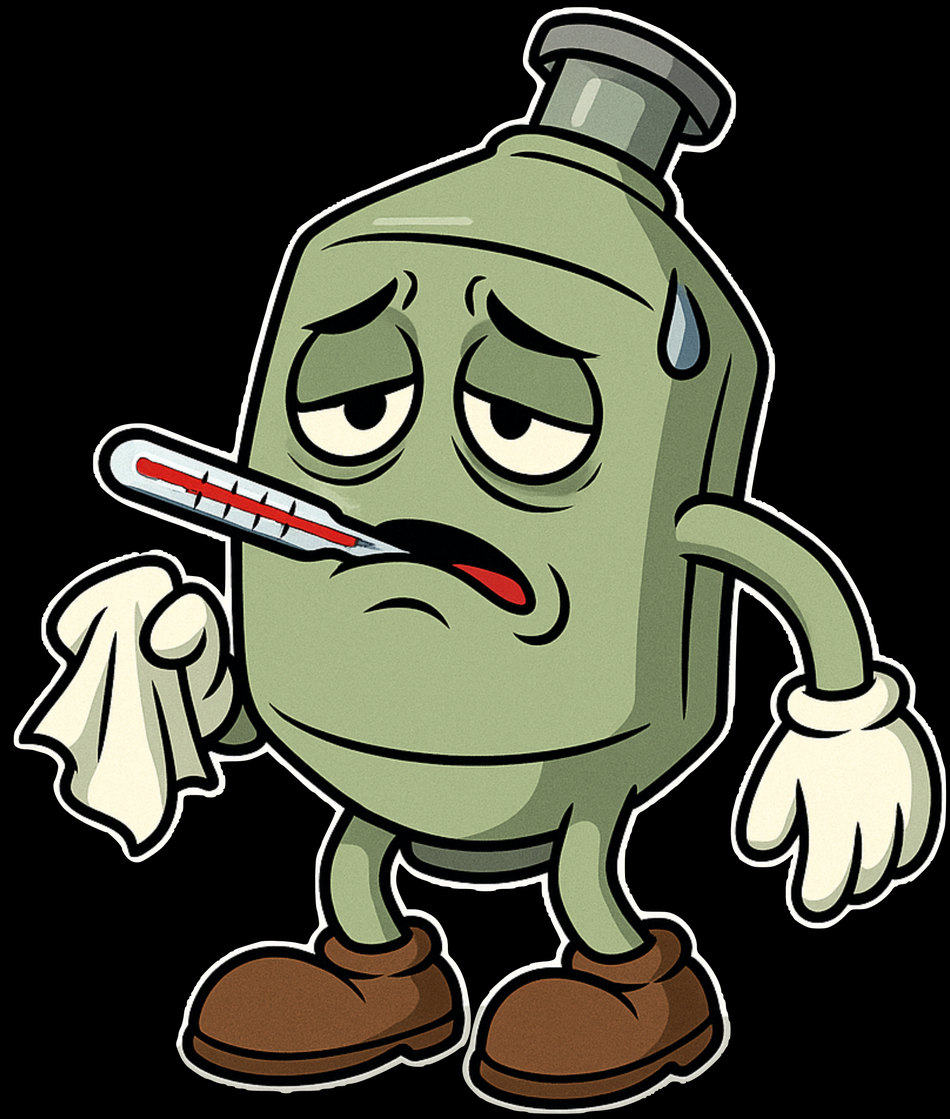
HaKCing OBD-II Emissions Testing

DEF CON 33

Archwisp - August 2025



The thing about rotary motors is that they kill catalytic converters.



“Kansas City, MO, and the surrounding areas **do not require emissions testing**.”

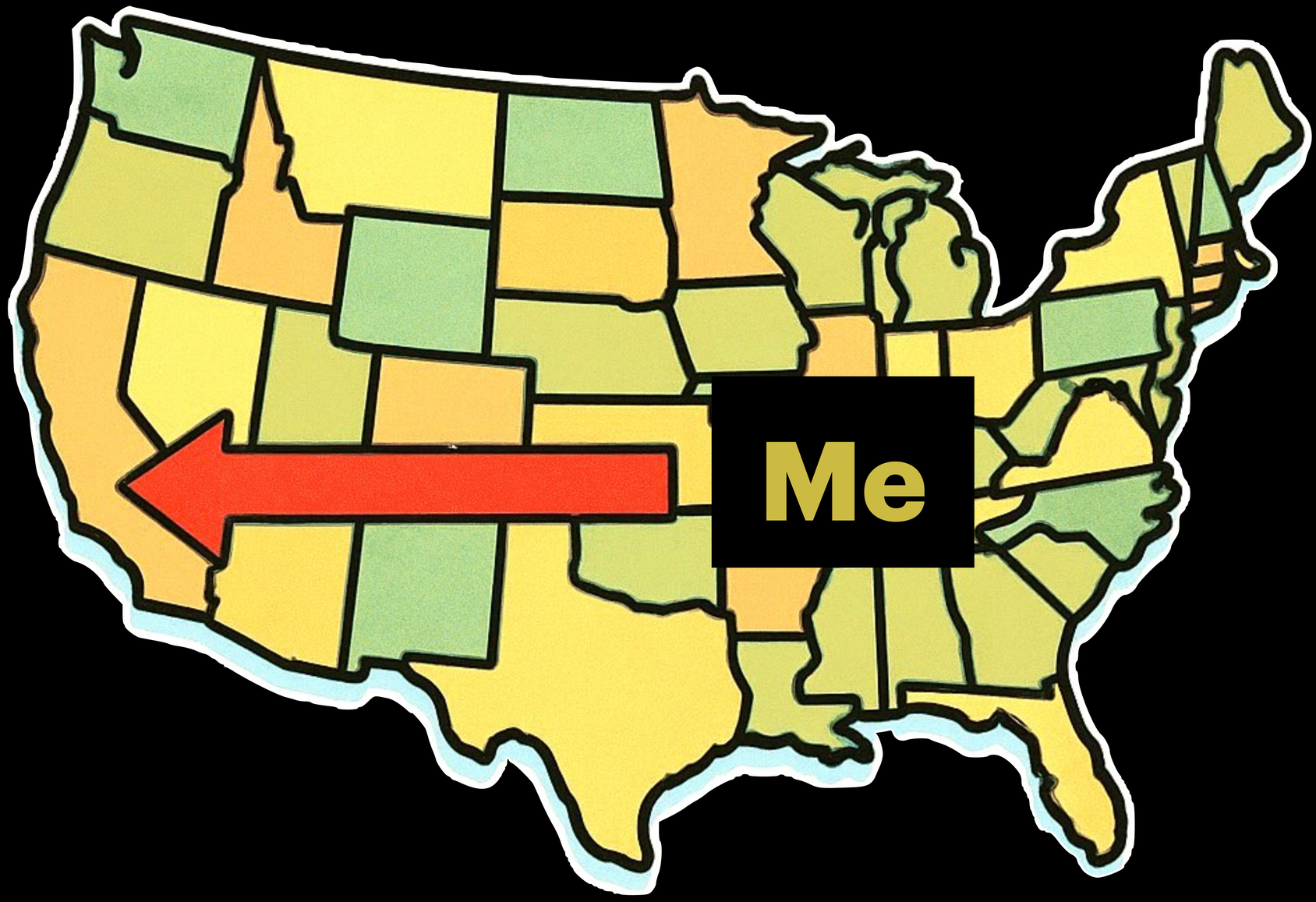
Rip it out!








The next 8 years


Me

"Vehicle **emissions testing is required** in major metropolitan areas…"



"Statute authorizes the Director of **** to **exempt certain vehicles**, including collectible vehicles, **from vehicle emissions requirements**."



"… **primarily for use in car club activities**, exhibitions, parades … **and be used only infrequently** …"



"... and **requires the owner to have another vehicle** for personal use."


SPACE RANGER
LIGHTYEAR

Welp.

Glad I kept those parts.



YEAR / MAKE	2004 MAZDA	GVWR WGT GROUP	0-4000	FUEL TYPE	GASOLINE

OBD READINESS MONITORS STATUS

CATALYST	NOT READY	EVAP SYSTEM	NOT READY
HEATED CAT	NOT SUPPORTED	O2 SENSOR	NOT READY	AIR SYSTEM	NOT READY
EGR	NOT SUPPORTED	HEATED O2	READY	AIR CONDITIONER	NOT SUPPORTED

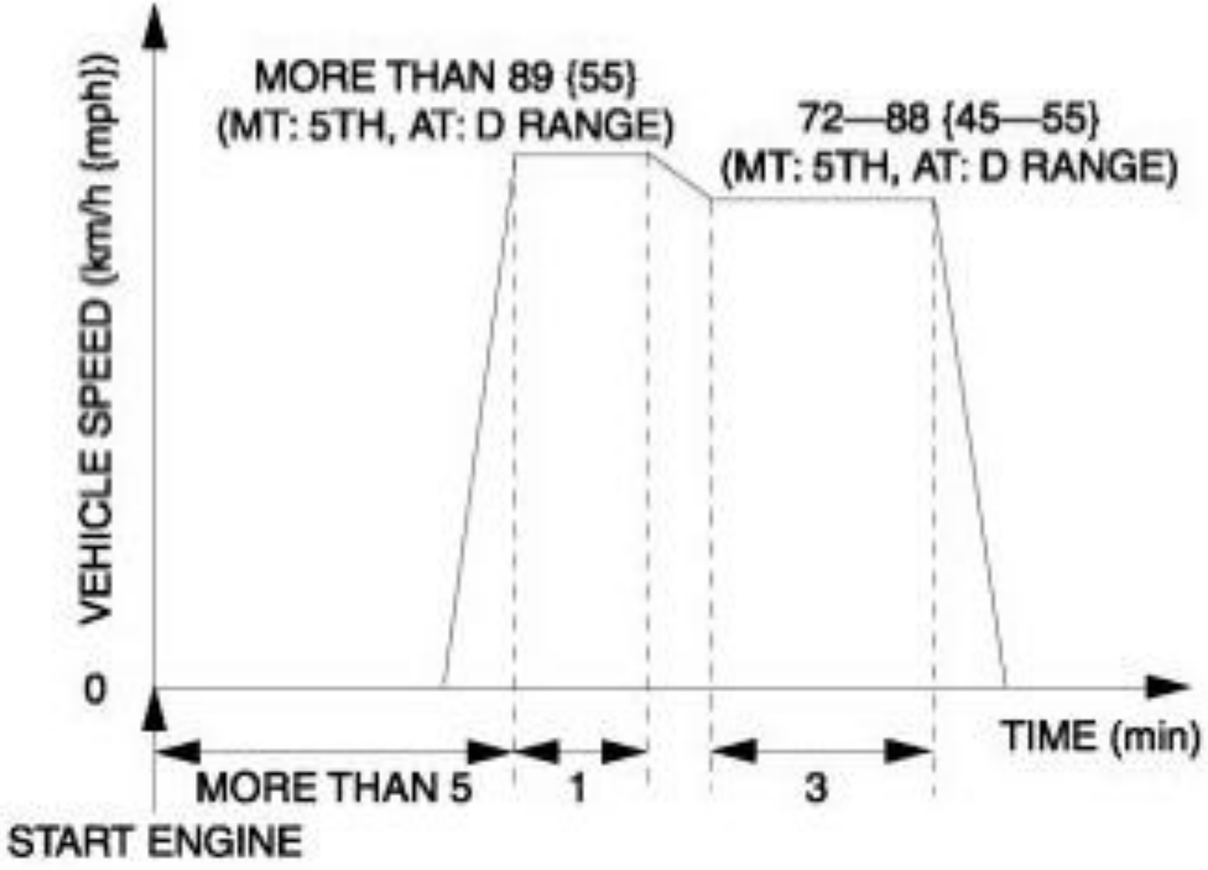
DESCRIPTION OF VEHICLE REJECTION REASON

IN PREPARING TO INSPECT THIS VEHICLE, THE FOLLOWING ITEM(S) PREVENTED THE INSPECTION FROM BEING COMPLETED:

- THE VEHICLE'S COMPUTER SYSTEM IS "NOT READY" TO BE TESTED AS REPORTED.

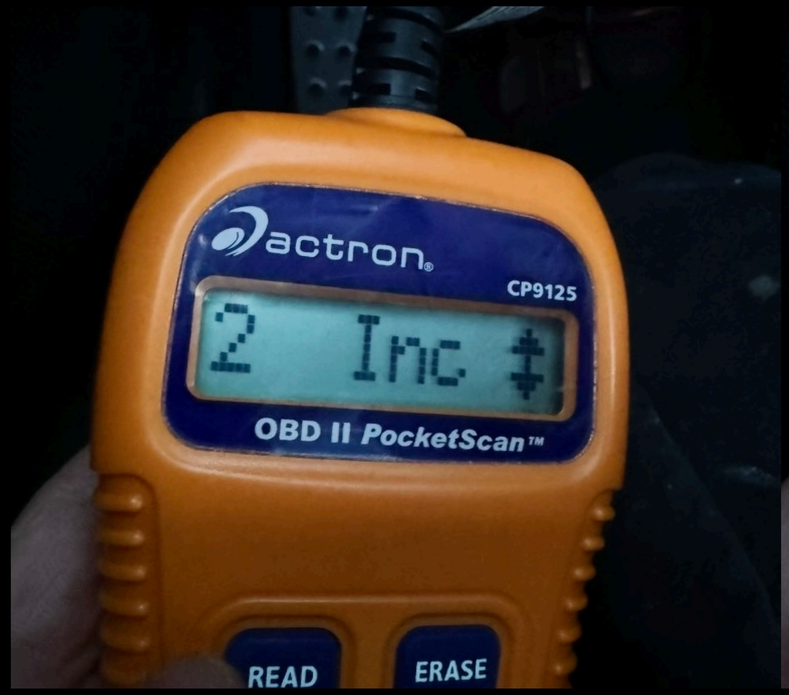
Mode 3 (HO2S heater, HO2S, and TWC Repair Verification Drive Mode)

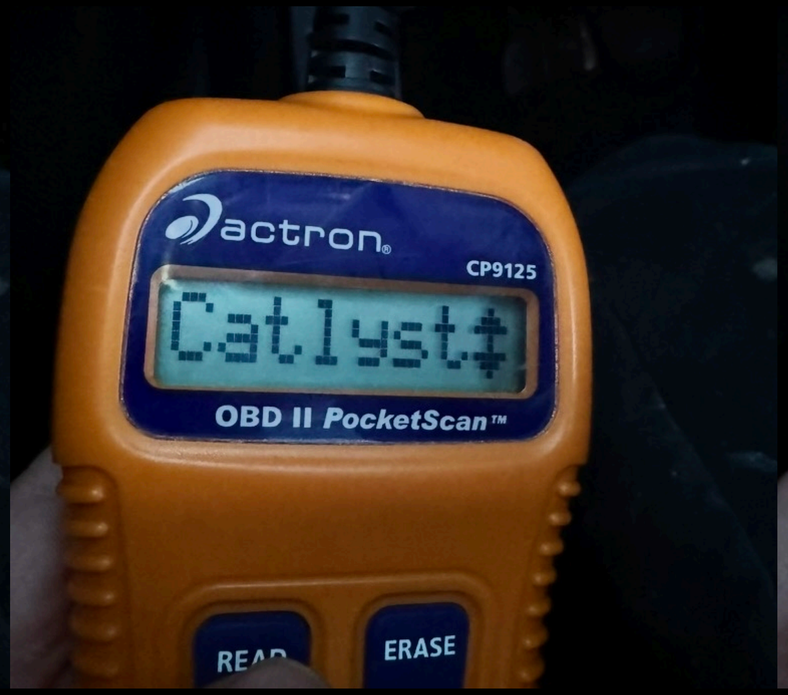
1. Perform the Mode 1 first.
2. Verify that all accessory loads (A/C, headlights, blower fan, rear window defroster) are off.
3. Drive the vehicle as shown in the graph. The driving condition before driving at constant spee specified.

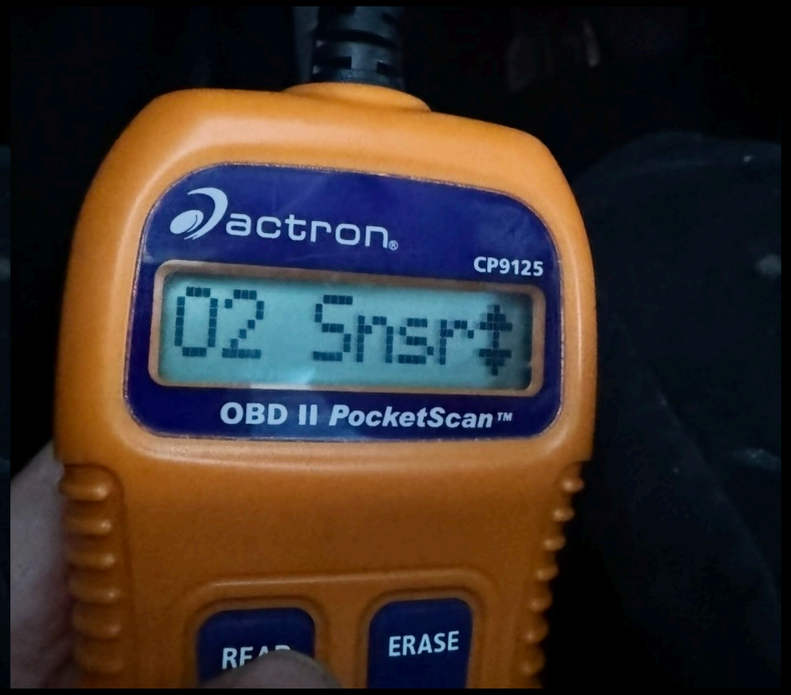



ONE
ETERNITY
LATER

!@#$


actron
CP9125
2 Inc
OBD II PocketScan™
READ
ERASE


actron
CP9125
Catlyst
OBD II PocketScan™
ERASE


actron
CP9125
02 Snsr
OBD II PocketScan™
ERASE



DEF CON 26

How to draw an Owl.

"A fun and creative guide for beginners"



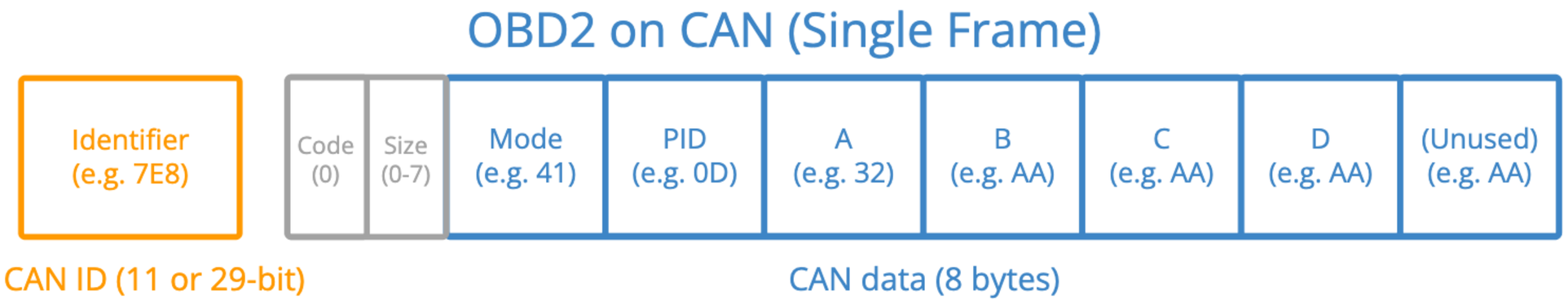
Fig 1. Draw two circles



Fig 2. Draw the rest of the damn Owl

The OBD2 diagnostic message [SAE J1979, ISO 15031-5]

To better understand OBD2 on CAN, let us consider a raw 'Single Frame' OBD2 CAN message. In simplified terms, an OBD2 message is comprised of an identifier, data length (PCI field) and data. The data is split in Mode, parameter ID (PID) and data bytes.



https://www.csselectronics.com/pages/obd2-explained-simple-intro

Legislated OBD CAN identifiers (11-bit)

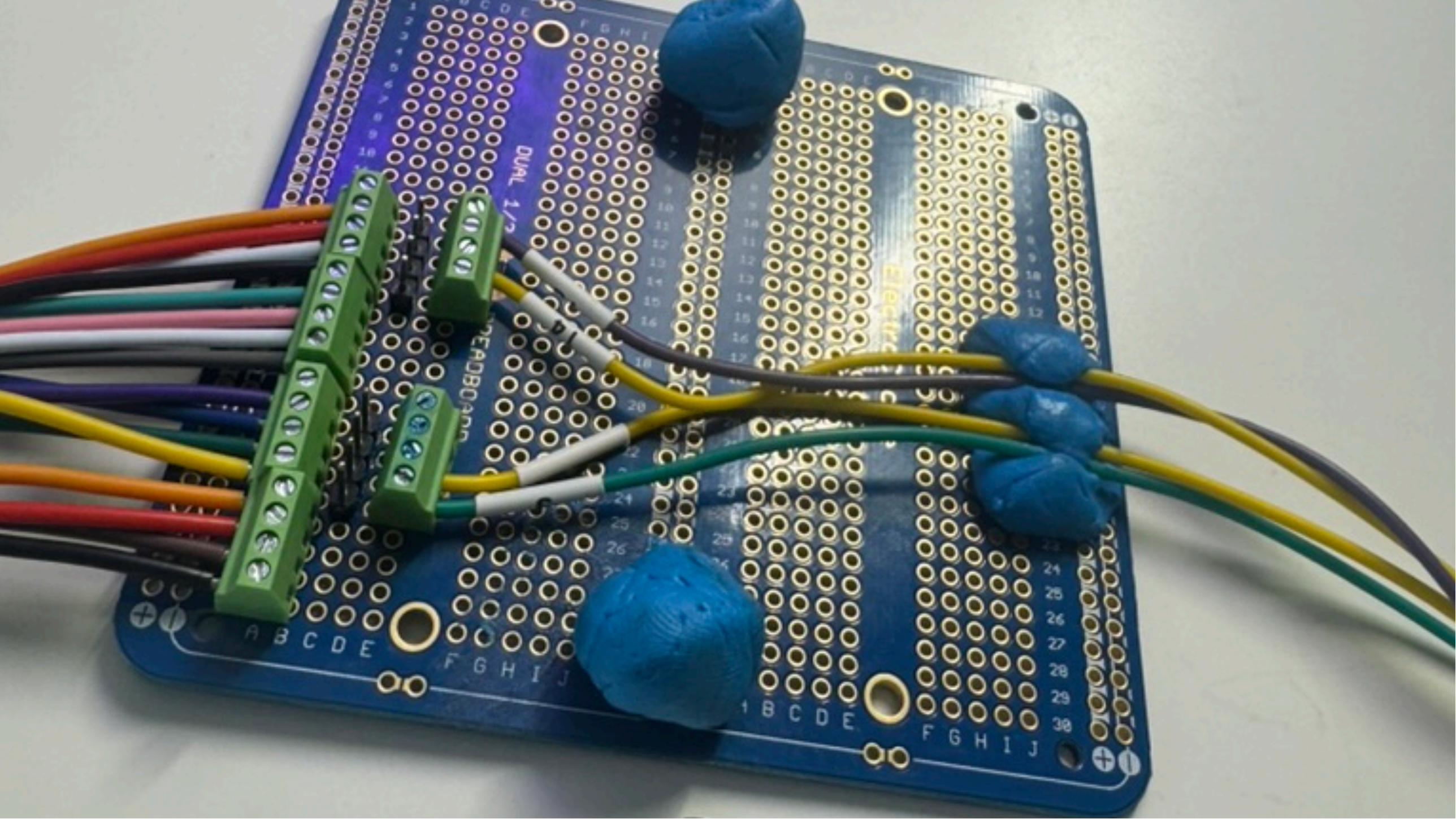
CAN ID	Description
0x7DF	Functionally addressed request sent by tester
0x7E0 to 0x7E7	Physical request from tester to ECU #1 to #8
0x7E8 to 0x7EF	Physical response from ECU #1 to #8 to tester

Legislated OBD CAN identifiers (29-bit)

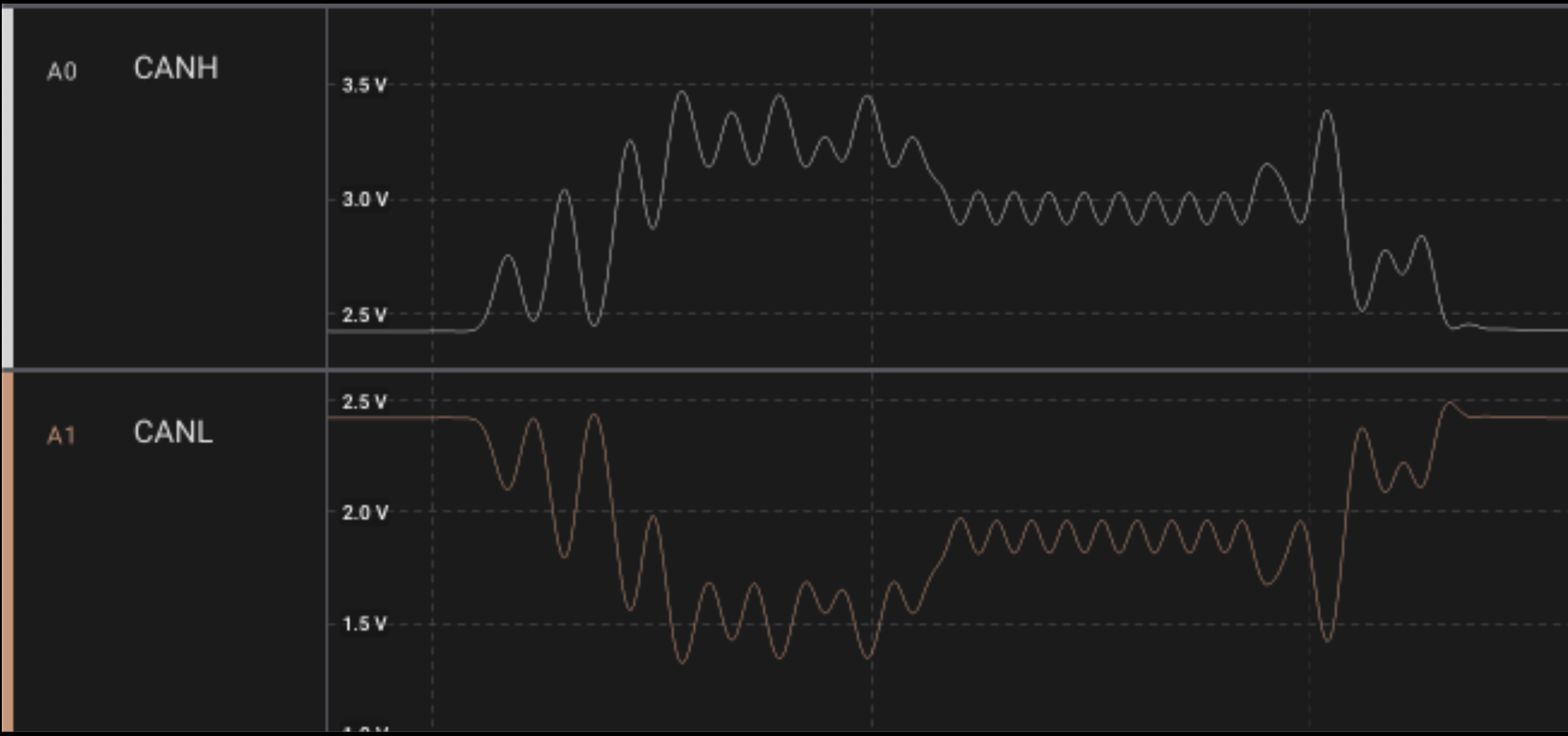
CAN ID	Description
0x18DB33F1	Functionally addressed request sent by tester
0x18DAxxF1	Physical request from tester to ECU #xx
0x18DAF1xx	Physical response from ECU #xx to tester

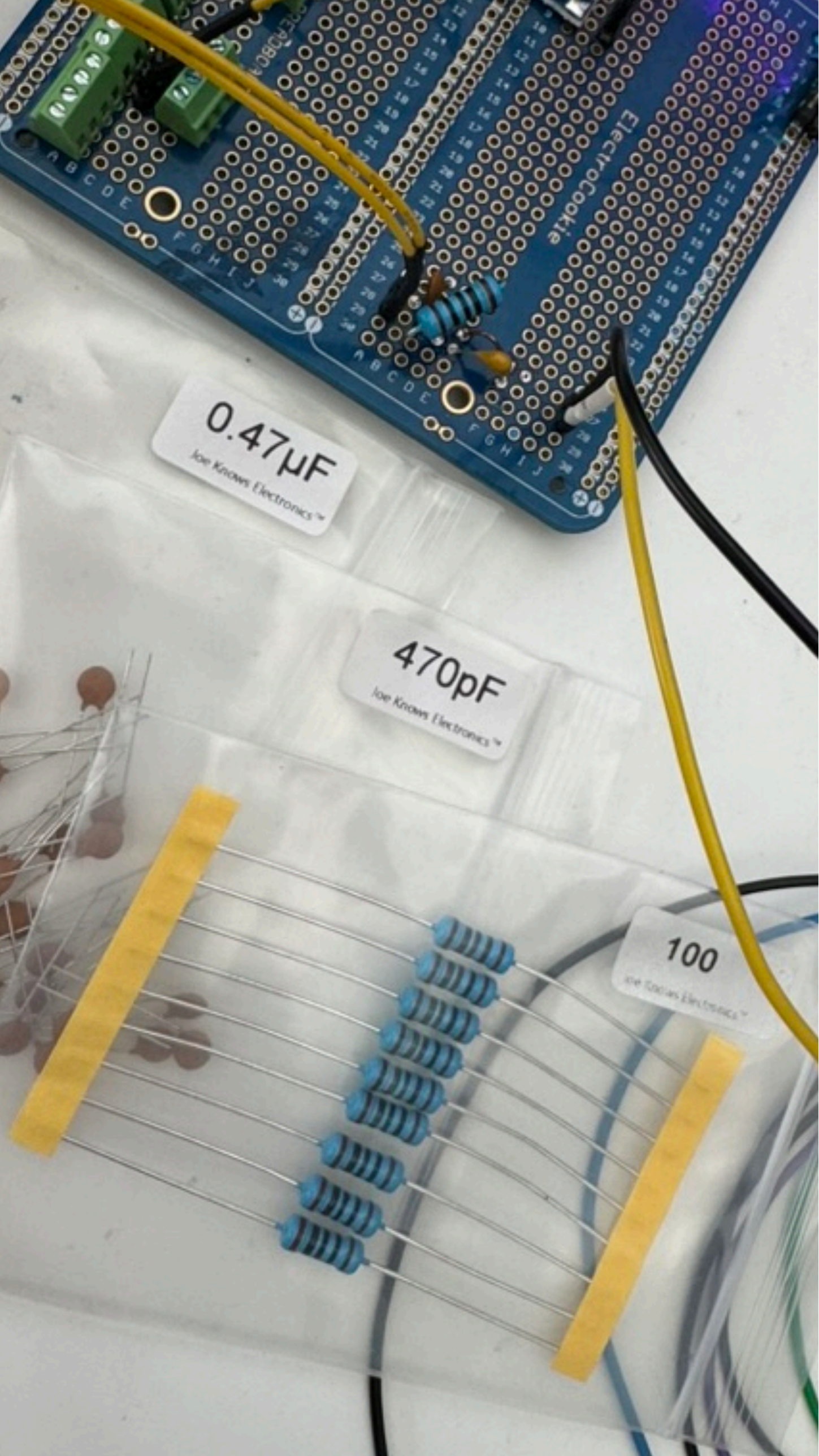
https://www.csselectronics.com/pages/obd2-explained-simple-intro

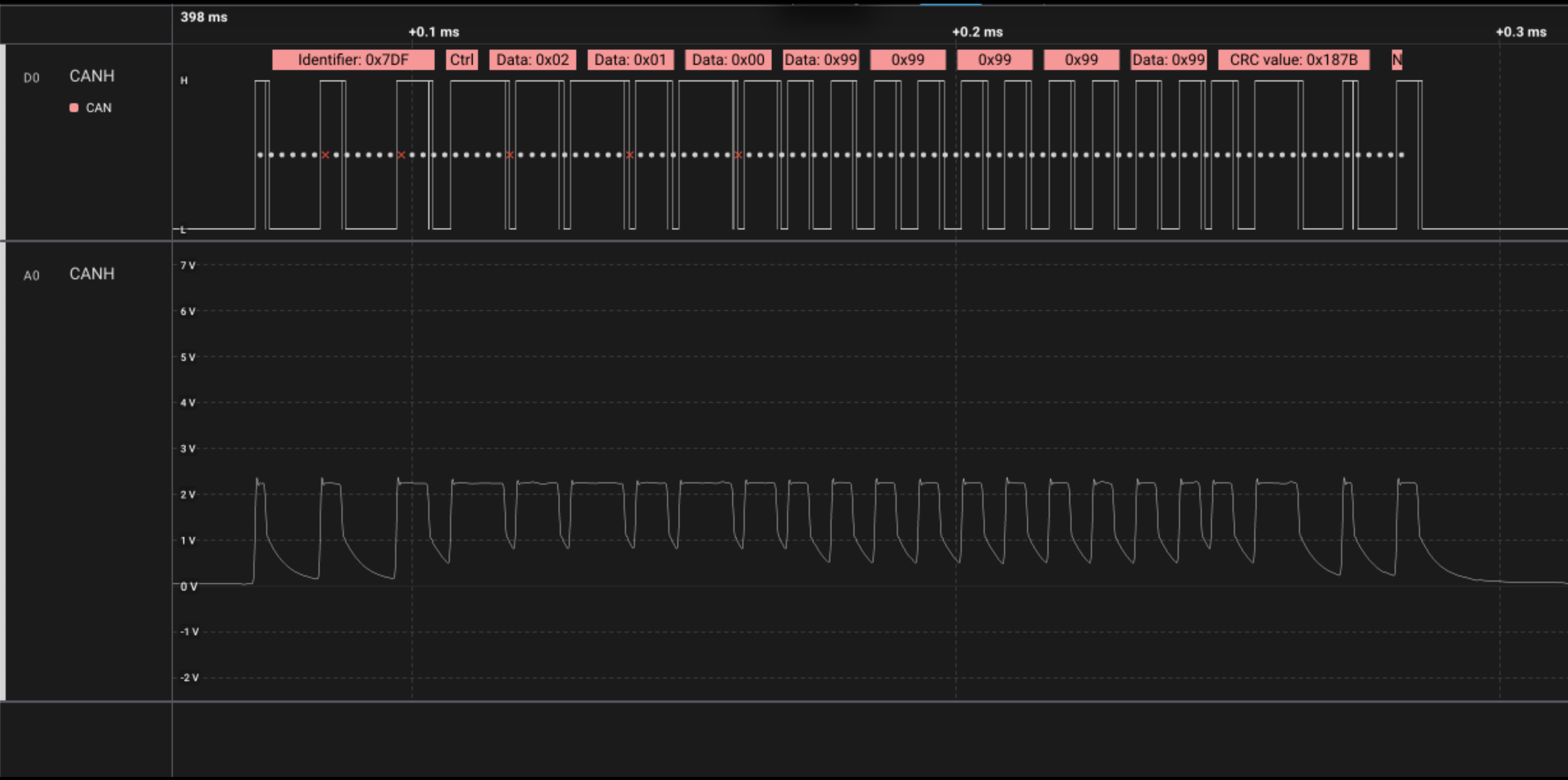


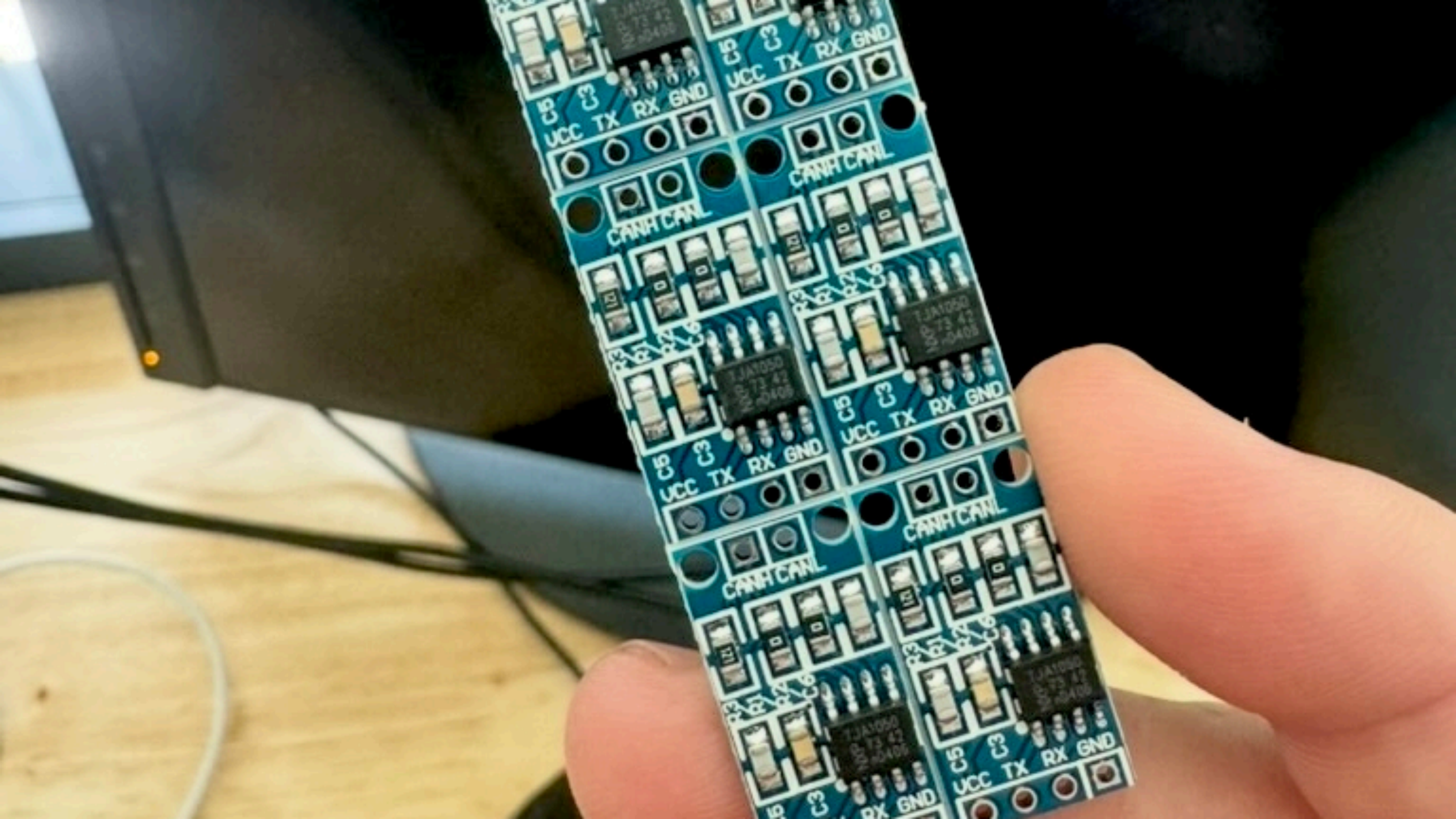

DUAL 1/2
A B C D E
F G H I J
1 B C D E
F G H I J
24
25
26
27
28
29
30


actron
CP9125
OBD II PocketScan™
READ
ERASE

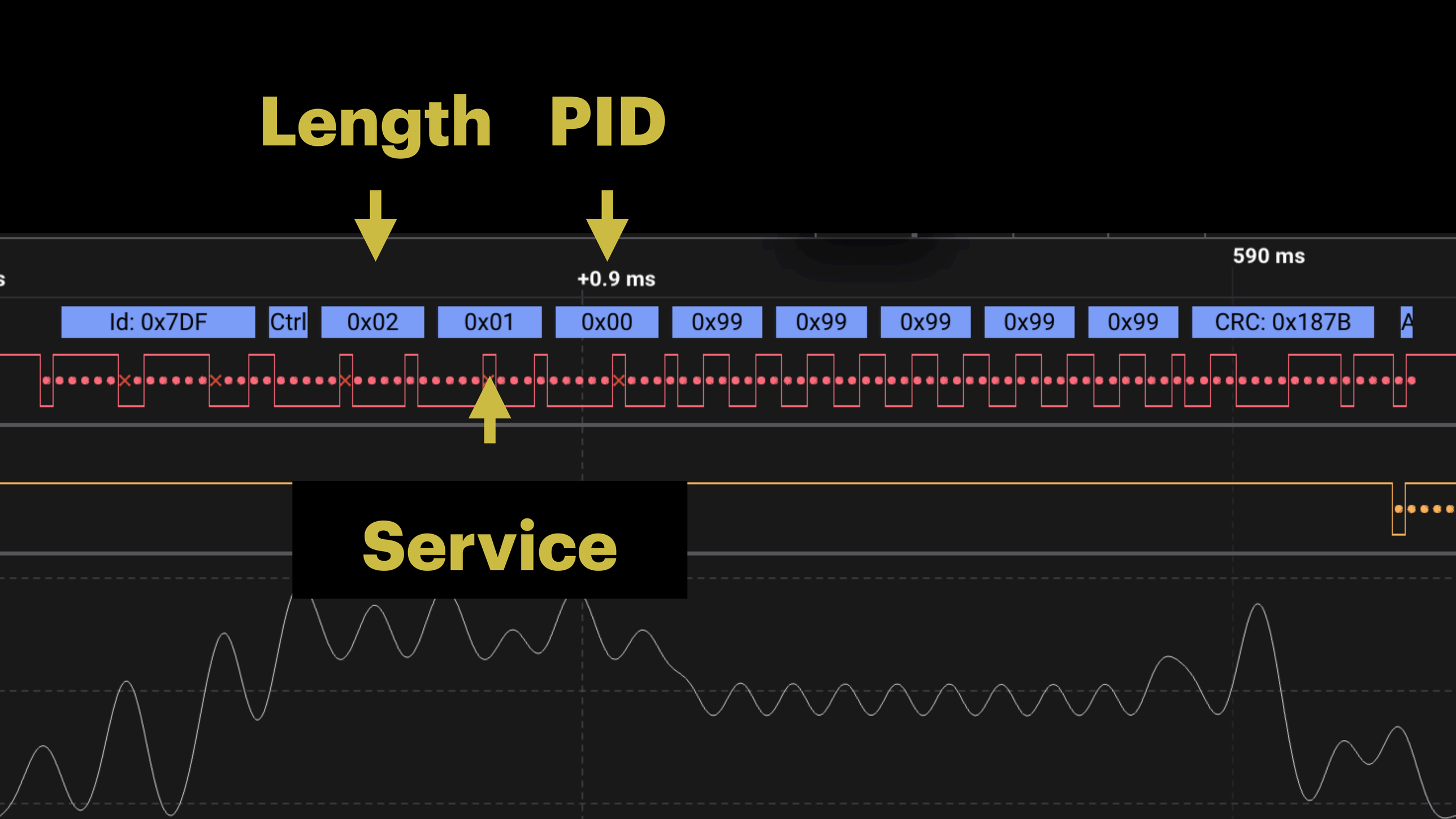

A0
CANH
3.5 V
3.0 V
2.5 V
A1
CANL
2.5 V
2.0 V
1.5 V


0.47µF
Joe Knows Electronics™
470pF
Joe Knows Electronics™
100


398 ms
+0.1 ms
+0.2 ms
+0.3 ms
D0
CANH
CAN
Identifier: 0x7DF
Ctrl
Data: 0x02
Data: 0x01
Data: 0x00
Data: 0x99
0x99
0x99
0x99
Data: 0x99
CRC value: 0x187B
N
H
L
A0
CANH
7 V
6 V
5 V
4 V
3 V
2 V
1 V
0 V
-1 V
-2 V


VCC TX RX GND
CANH CANL


+0.8 ms
+0.9 ms
+0.1 ms
D2
RX
CAN RX
Id: 0x7DF
Ctrl
0x02
0x01
0x00
0x99
0x99
0x99
0x99
0x99
CRC: 0x187B
A
H
L
D3
TX
CAN TX
H
L
A0
CANH
3.5 V
3.0 V
2.5 V
A1
CANL
2.5 V
2.0 V
1.5 V
A2
RX
4 V
2 V
0 V
A3
TX
5.0 V
4.5 V
4.0 V
3.5 V


Length
PID
+0.9 ms
590 ms
Id: 0x7DF
Ctrl
0x02
0x01
0x00
0x99
0x99
0x99
0x99
0x99
CRC: 0x187B
Service

Service 01 - Show current data [edit]

PIDs (hex)	PID (Dec)	Data bytes returned	Description	Min value	Max value	Units	Formula[a]
00	0	4	PIDs supported [$01 - $20]				Bit encoded [A7..D0] == [PID $01..PID $20] See below
01	1	4	Monitor status since DTCs cleared. (Includes malfunction indicator lamp (MIL), status and number of DTCs, components tests, DTC readiness checks)				Bit encoded. See below

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

HEX | 11-bit IDs

PID	Name	Bit start	Bit length	Scale	Offset	Min | Max	Unit
00	PIDs supported [01 - 20]	31	32	1	0		Encoded

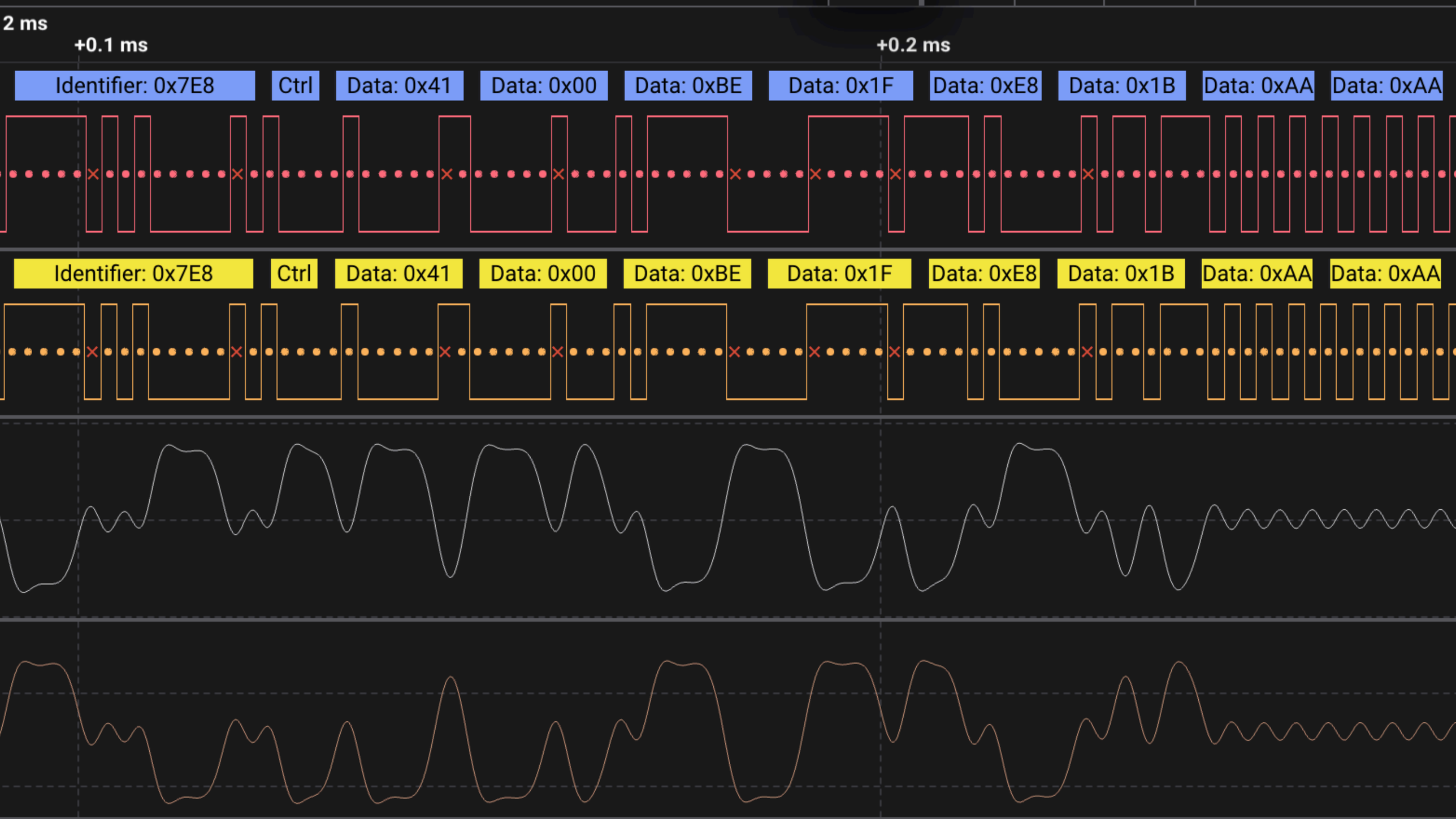
	CAN ID	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
Request	7DF	02	01	00	AA	AA	AA	AA	AA
Response (example)	7E8	06	41	00	12	34	56	78	AA

Physical value (DEC) = 0 + 1 * 305419896 = **305419896** **Encoded**

Physical value (BIN) = 00010010000110100010101100111000

PID	Name	Supported?
01	Monitor status since DTCs cleared	No
02	Freeze DTC	No
03	Fuel system status	No

https://www.csselectronics.com/pages/obd2-pid-table-on-board-diagnostics-j1979


2 ms
+0.1 ms
+0.2 ms
Identifier: 0x7E8
Ctrl
Data: 0x41
Data: 0x00
Data: 0xBE
Data: 0x1F
Data: 0xE8
Data: 0x1B
Data: 0xAA
Data: 0xAA
Identifier: 0x7E8
Ctrl
Data: 0x41
Data: 0x00
Data: 0xBE
Data: 0x1F
Data: 0xE8
Data: 0x1B
Data: 0xAA
Data: 0xAA


+0.2 ms
+0.3 ms
+0.4 ms
D2
RX
CAN RX
H
L
E
E
D3
TX
CAN TX
H
L
E
E
A0
CANH
4.0 V
3.5 V
3.0 V
2.5 V
A1
CANL
2.5 V
2.0 V
1.5 V
1.0 V


actron
CP9125
NO LINK
OBD II PocketScan™
READ
ERASE

Remember the owl?

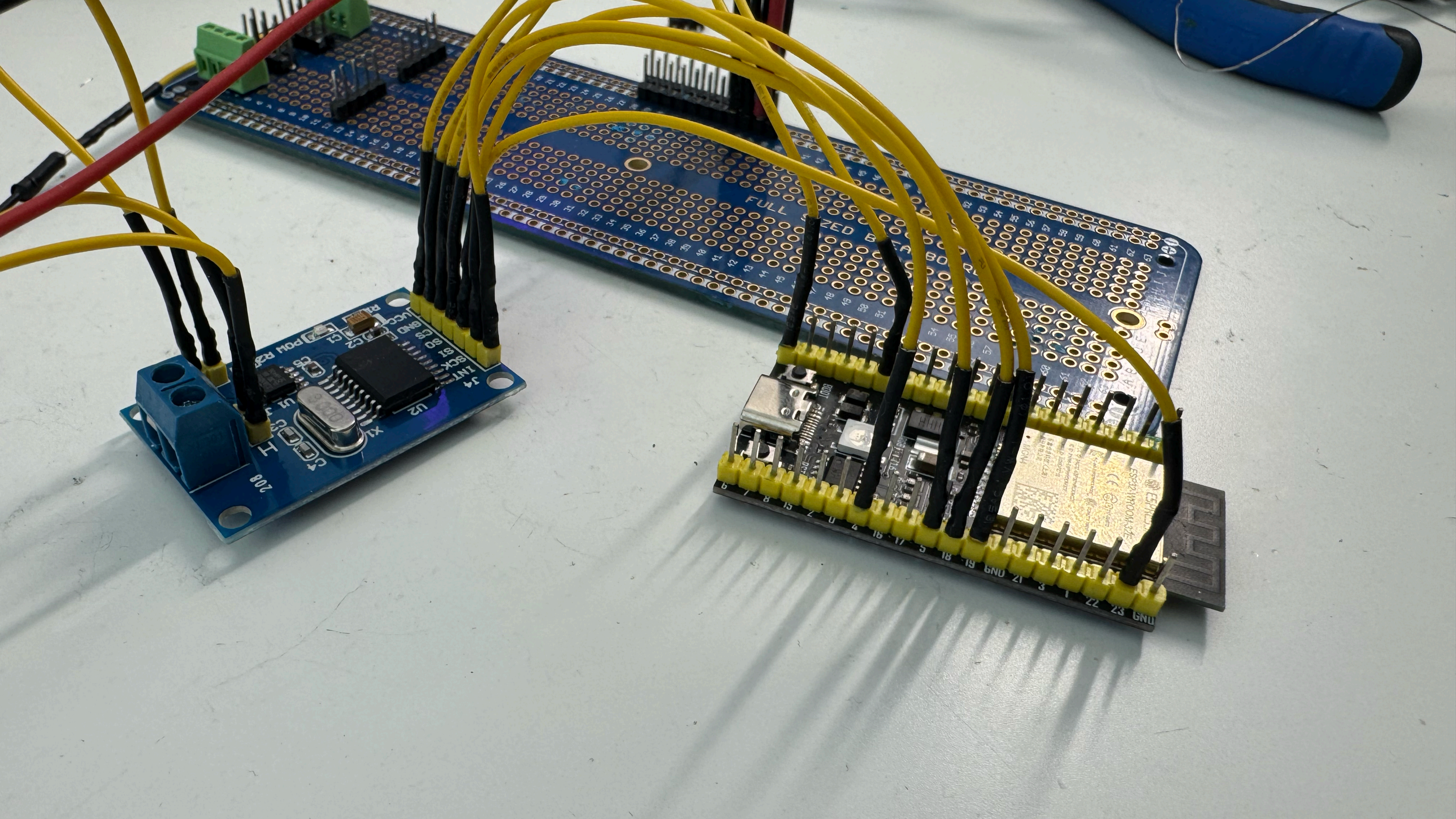
- Hardware
- Microcontroller drivers
- Protocols
- High-level logic

This is the point where my friends were making a lot of noise about AI coding agents.

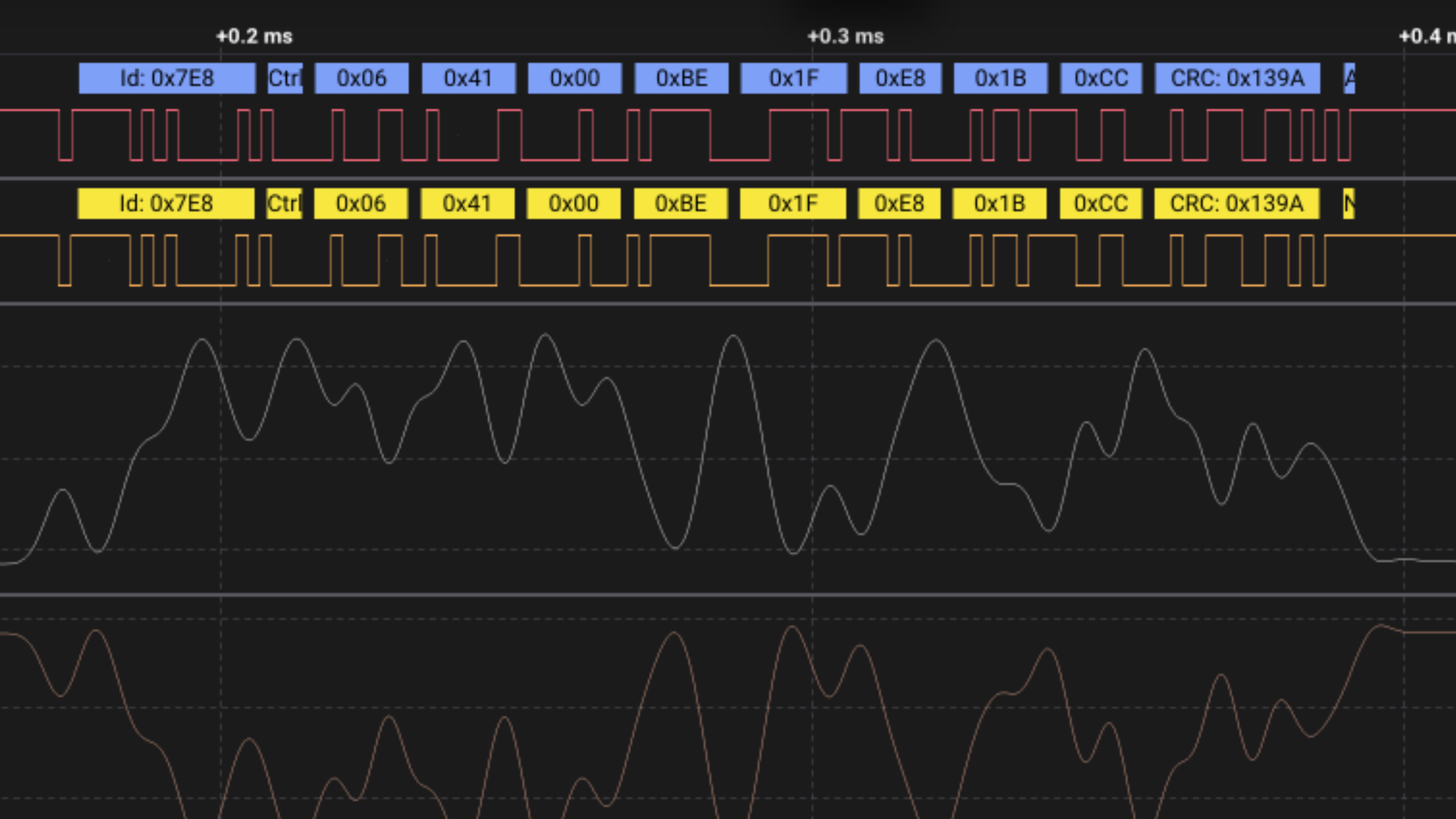


Things AI is good at

- Hardware ❌
- Microcontroller drivers ✅
- Protocols ❌
- High-level logic ❌


FULL
SIZED
208
INT
SCK
SI
SO
CS
GND
VCC
J4
U1
U2
X1
C1
C2
C3
R1
ESP32-WROOM-32E
GND
GND


ONE
ETERNITY
LATER


+0.2 ms
+0.3 ms
+0.4 m
Id: 0x7E8
Ctrl
0x06
0x41
0x00
0xBE
0x1F
0xE8
0x1B
0xCC
CRC: 0x139A
A
Id: 0x7E8
Ctrl
0x06
0x41
0x00
0xBE
0x1F
0xE8
0x1B
0xCC
CRC: 0x139A
N


actron
CP9125
0 Codes
OBD II PocketScan™
READ
ERASE

ALL MONITORS READY



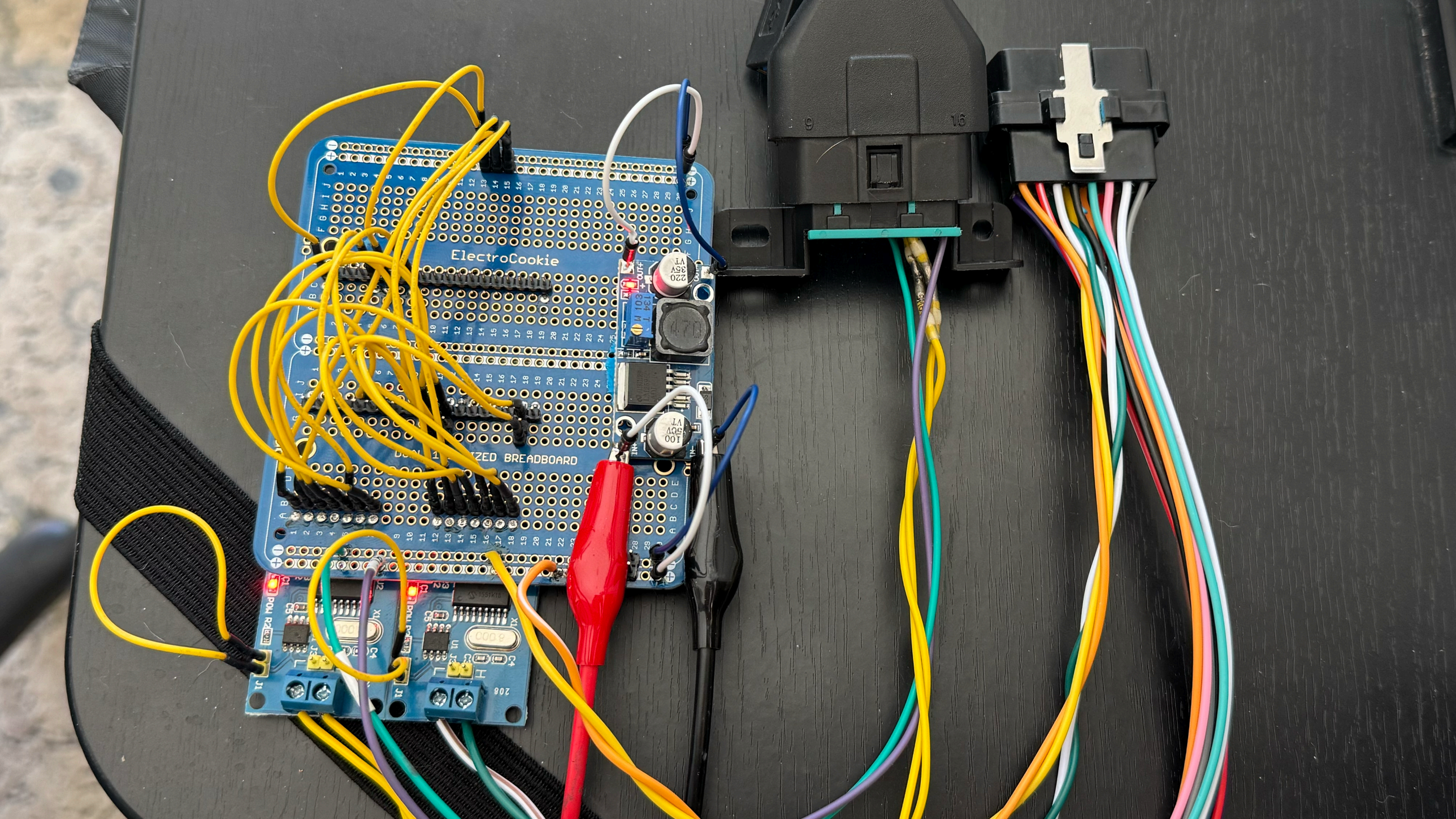




AI, please turn this into a proxy.






ElectroCookie
9
16


030531
6FE05

DEMO TIME

https://github.com/archwisp/OBD2Proxy