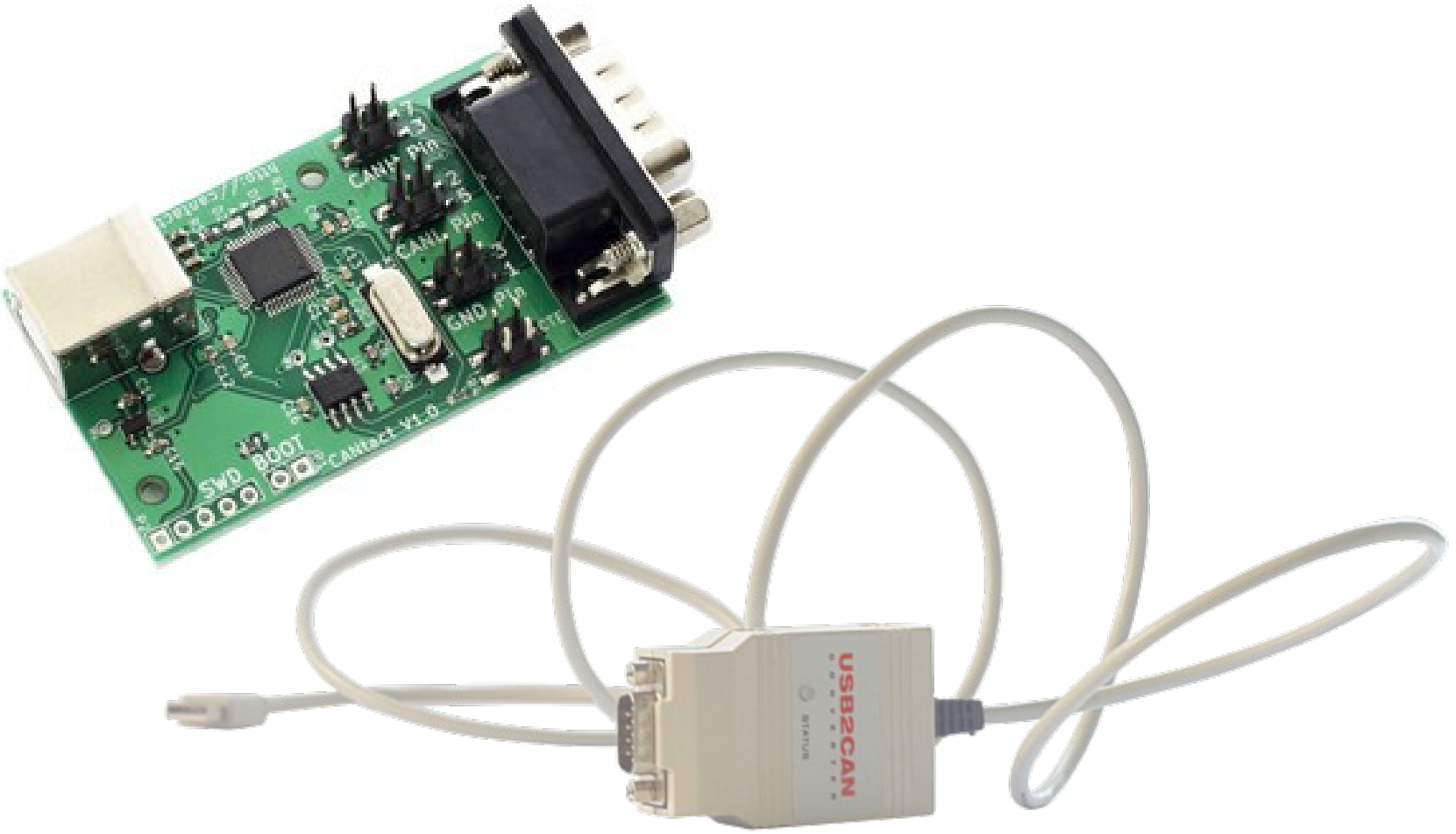
Howto Build an Auto Brothel

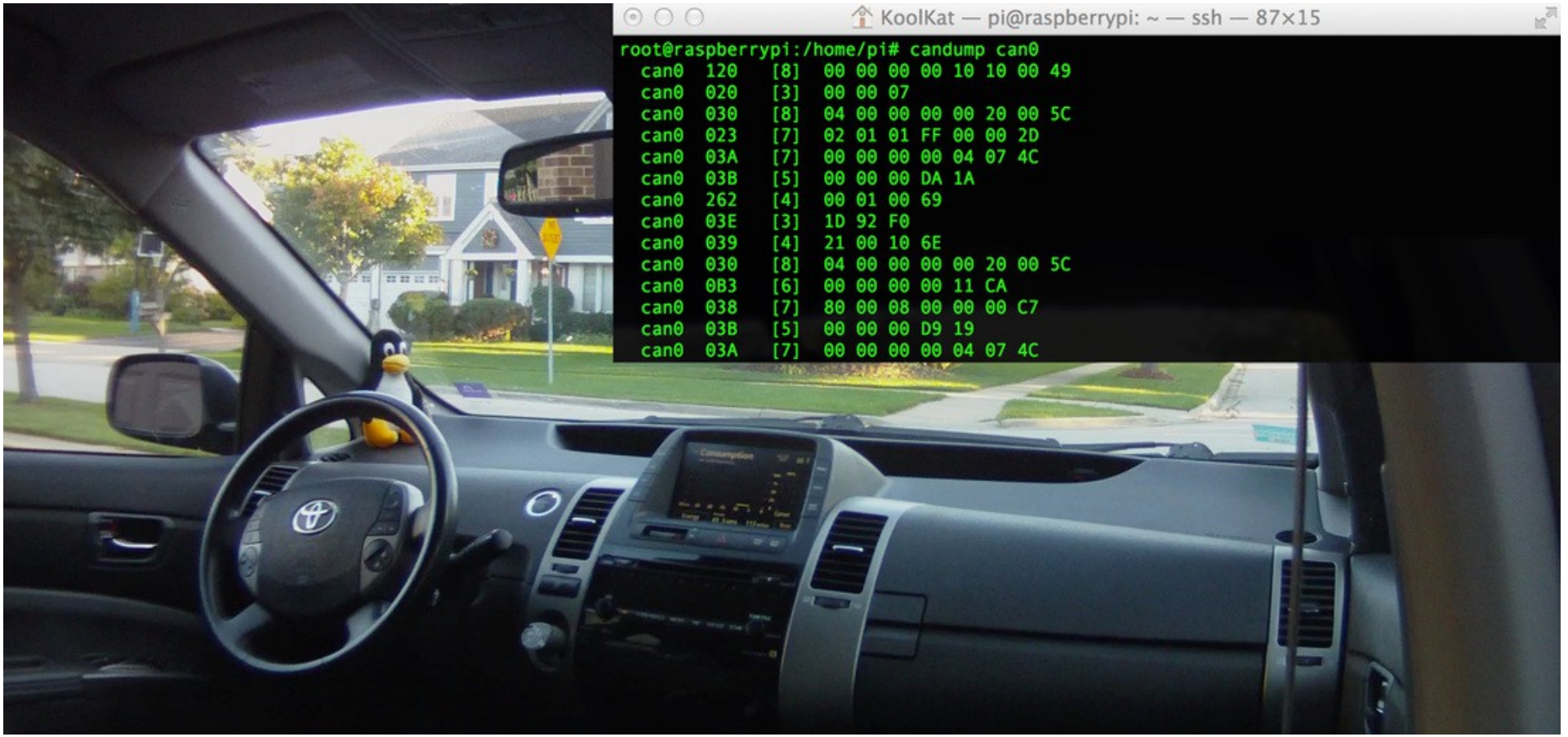
HW – CAN Bus (Cheap)



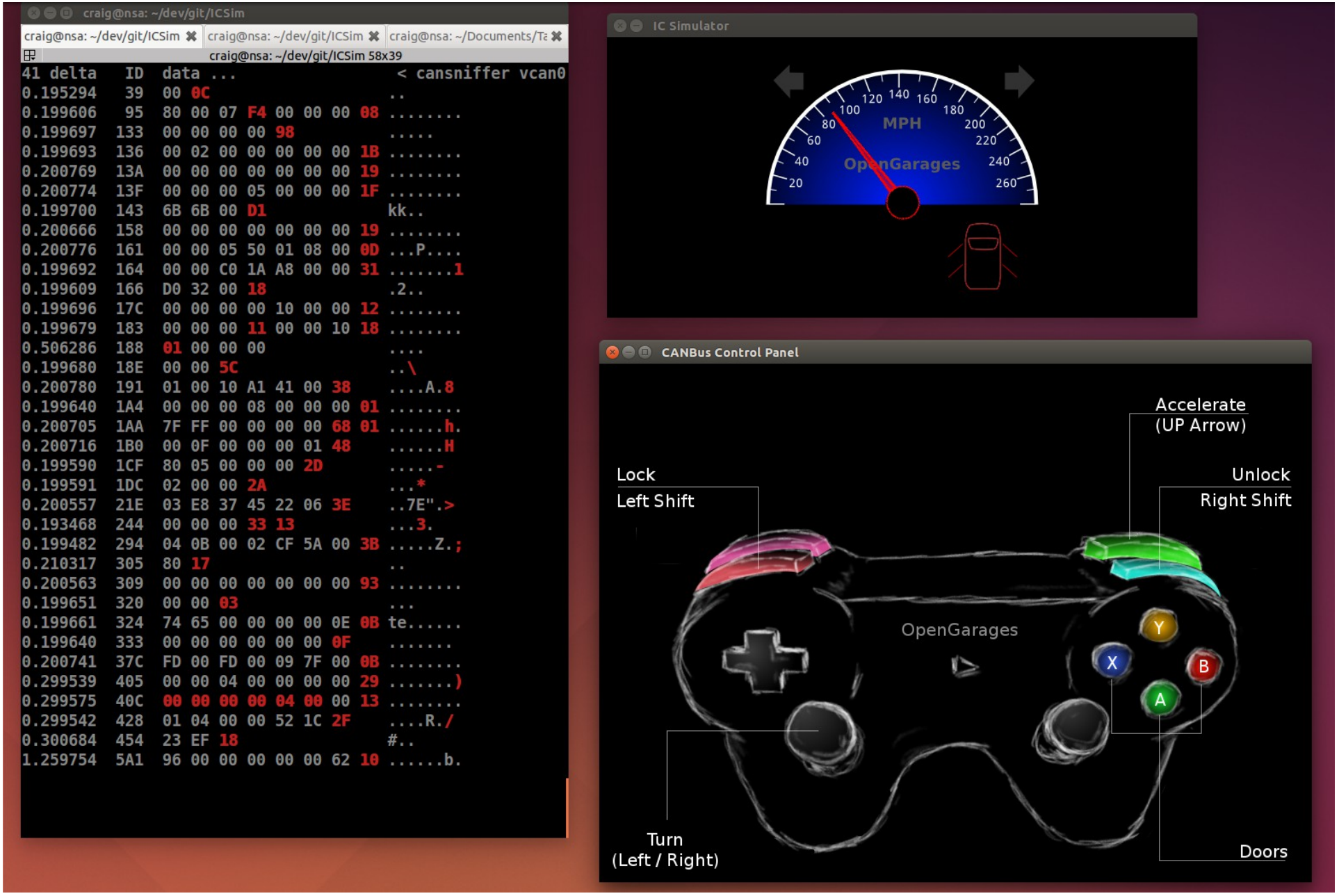
HW - Scantools

HW - Dealership Tools

SW - SocketCAN



SW – ICSim (not new but...)



UDS Server

- http://github.com/zombieCraig/uds-server

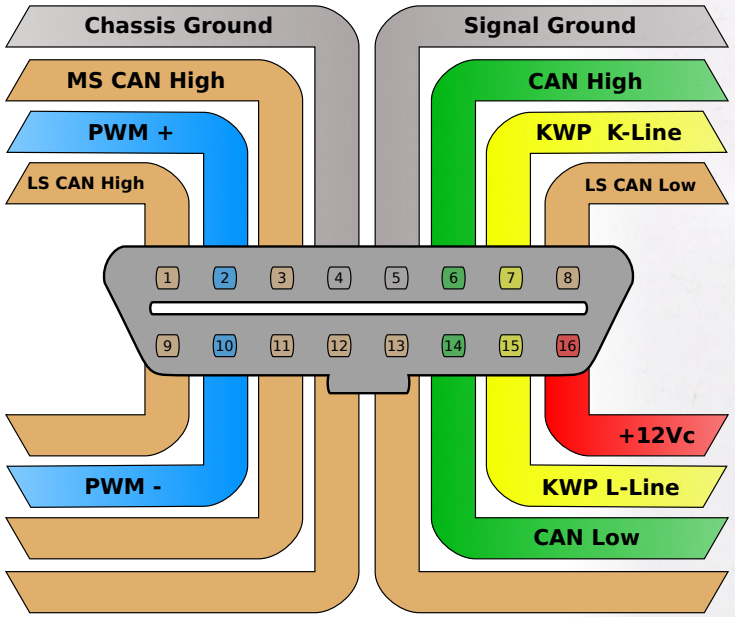
```
$ ./uds-server -h
Simulates UDS responses
Usage: ./uds-server [options] <can_interface>
    -z        Increase fuzz level
    -v        Verbose
    -l <logfile>     Log output to file instead of STDOUT
    -c        Don't fuzz ISOTP Spec, just data
    -F        Disable flow control (Functional Addressing)
    -V <vin>   Specify VIN (Default: WAUZZZ8V9FA149850)
```

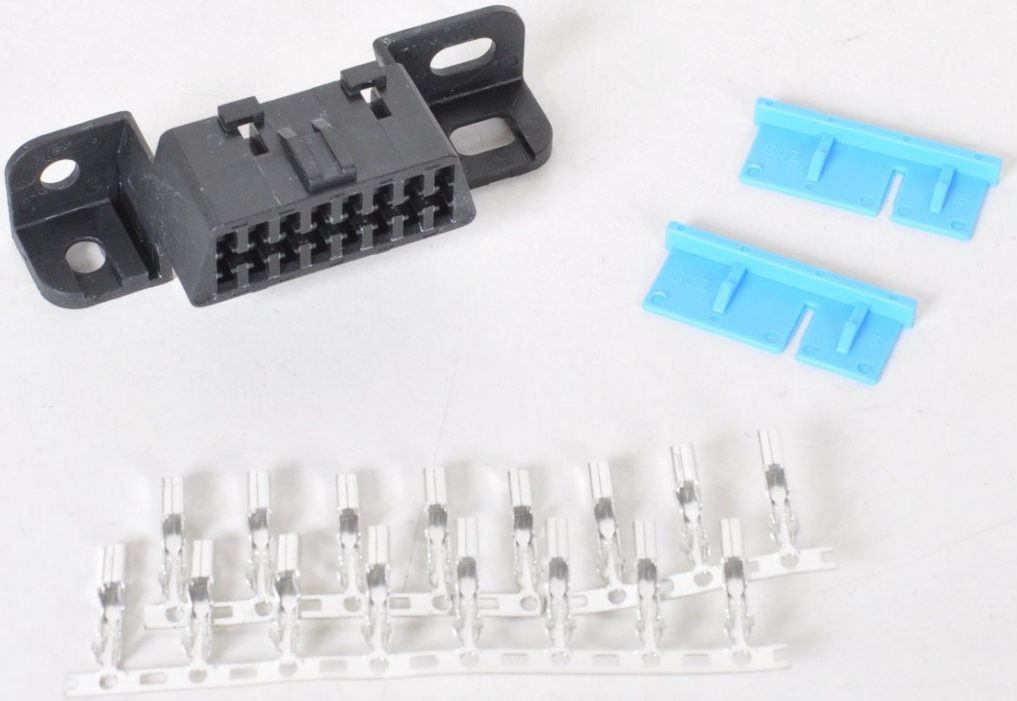
Introducing ODB GW

Howto build your own ODB GW

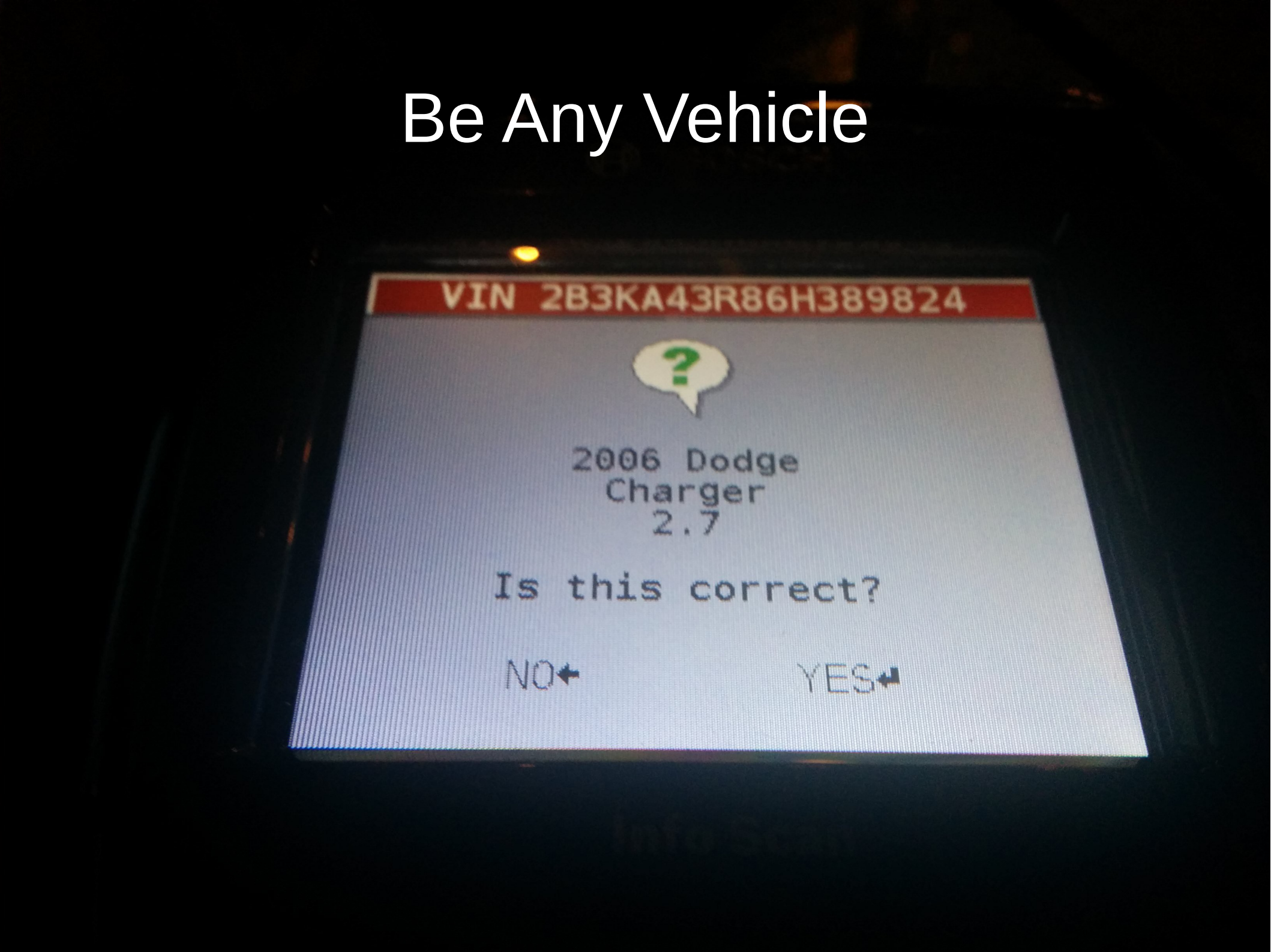
- 2 x Female J1962 ODB II Ports (~$10)
- Project Box (~$5)
- At least 2 120 ohm resistors (pennies)
- 12V power supply (~$12)

- Total: up to $25



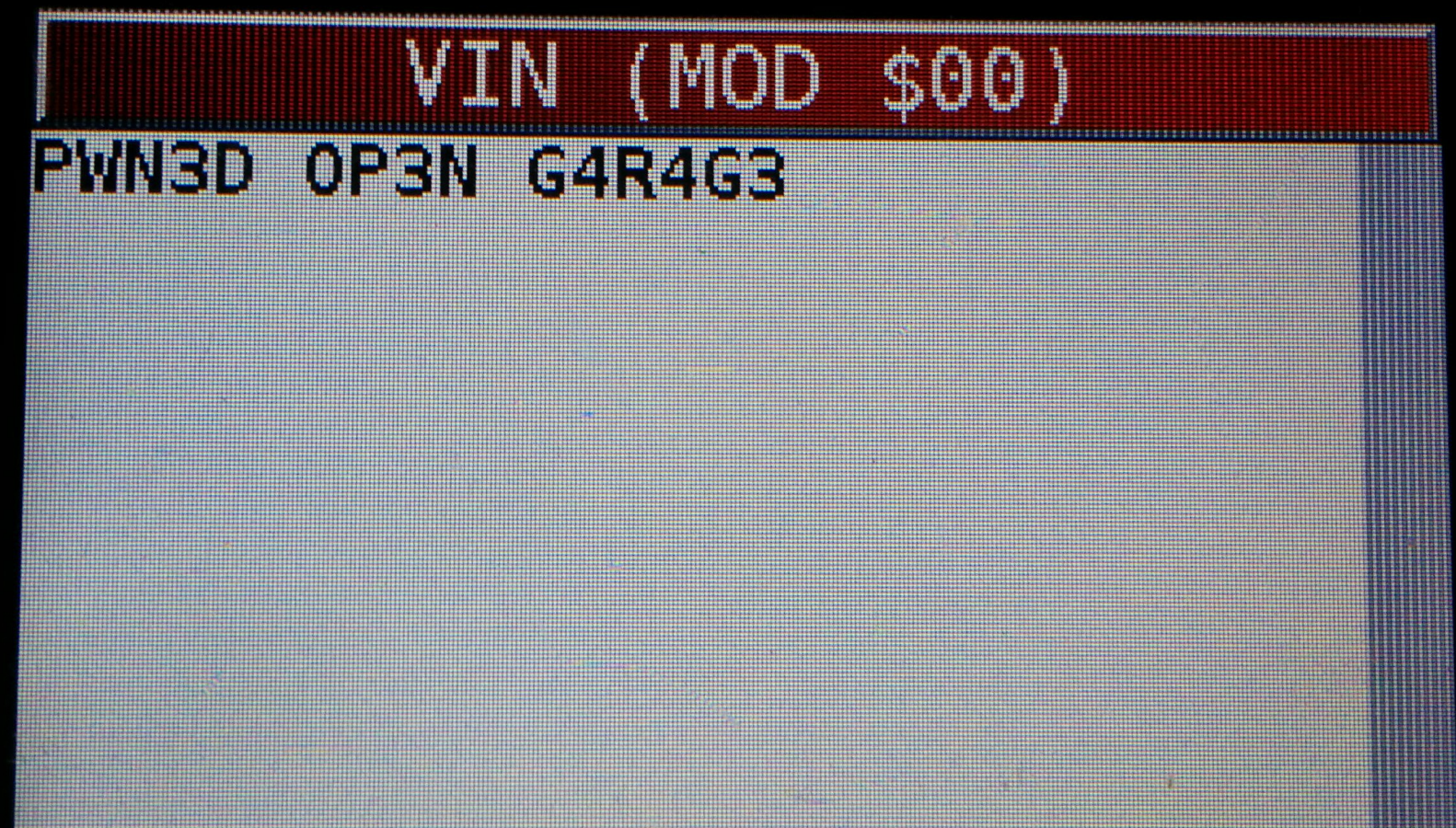


Be Any Vehicle



Have Any VIN

./uds-server -v -V "PWN3D OP3N G4R4G3" can0



Work from Anywhere

Quickly Identify I/O Controls

Pkt: 244#01 3E

Responding with a generic OK message

Pkt: 244#04 AA 03 02 07

Received GM Read Data by ID Request

+ Medium Rate

Pkt: 244#01 3E

Responding with a generic OK message

Pkt: 244#07 AE 01 03 00 00 00 00

Unhandled mode/sid: Device Control (GM)

Pkt: 244#01 3E

Responding with a generic OK message

Pkt: 101#FE 01 3E 55 55 55 55 55

Pkt: 244#01 3E

Responding with a generic OK message

Pkt: 244#02 AE 00

Unhandled mode/sid: Device Control (GM)

Pkt: 244#01 3E

Responding with a generic OK message

Pkt: 244#01 3E

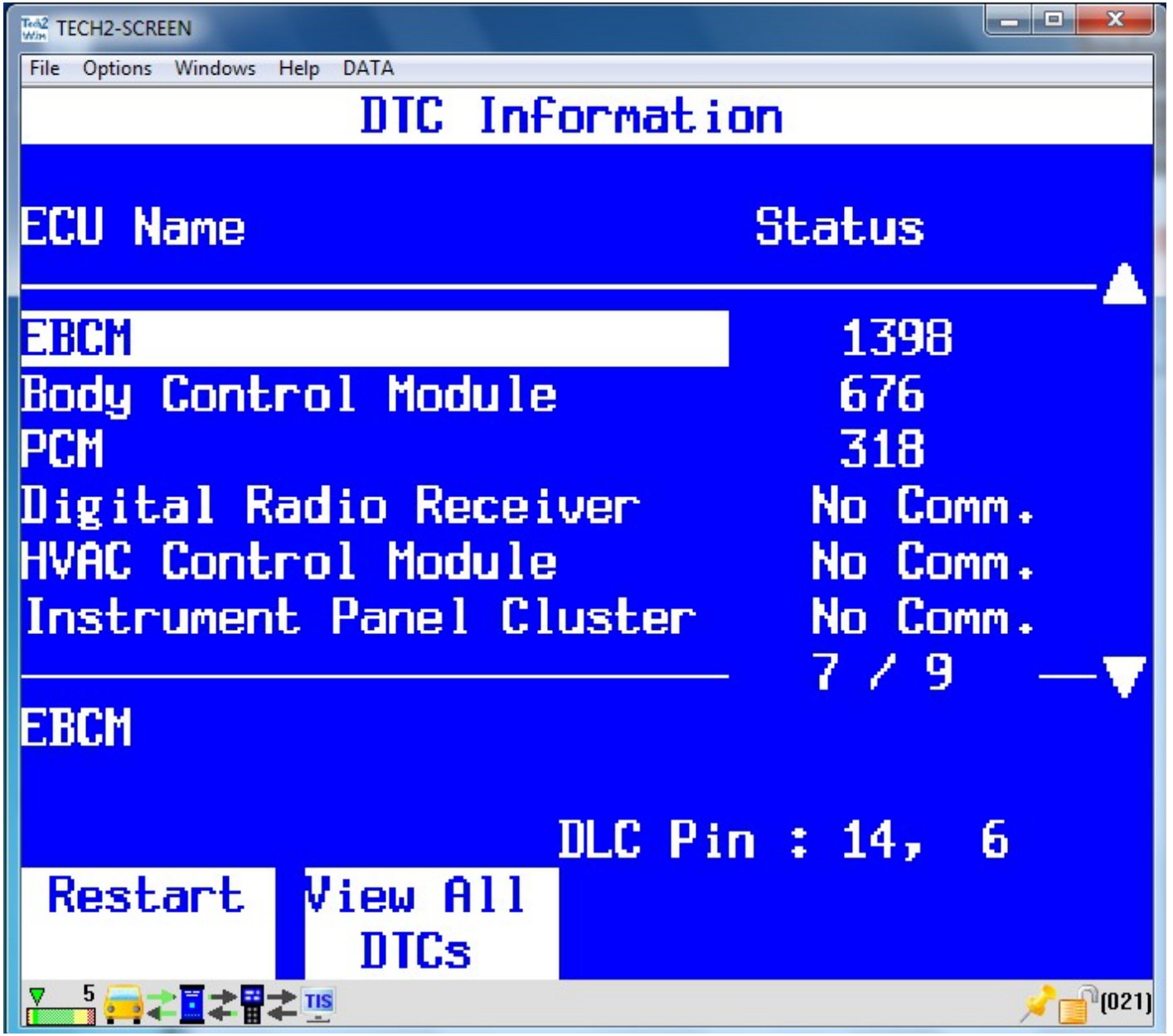
Responding with a generic OK message

Pkt: 244#02 AA 00

Received GM Read Data by ID Request

+ Stop Data Request

Exploit all the trust



Dealerships == squishy

Vehicle STDs

How to participate