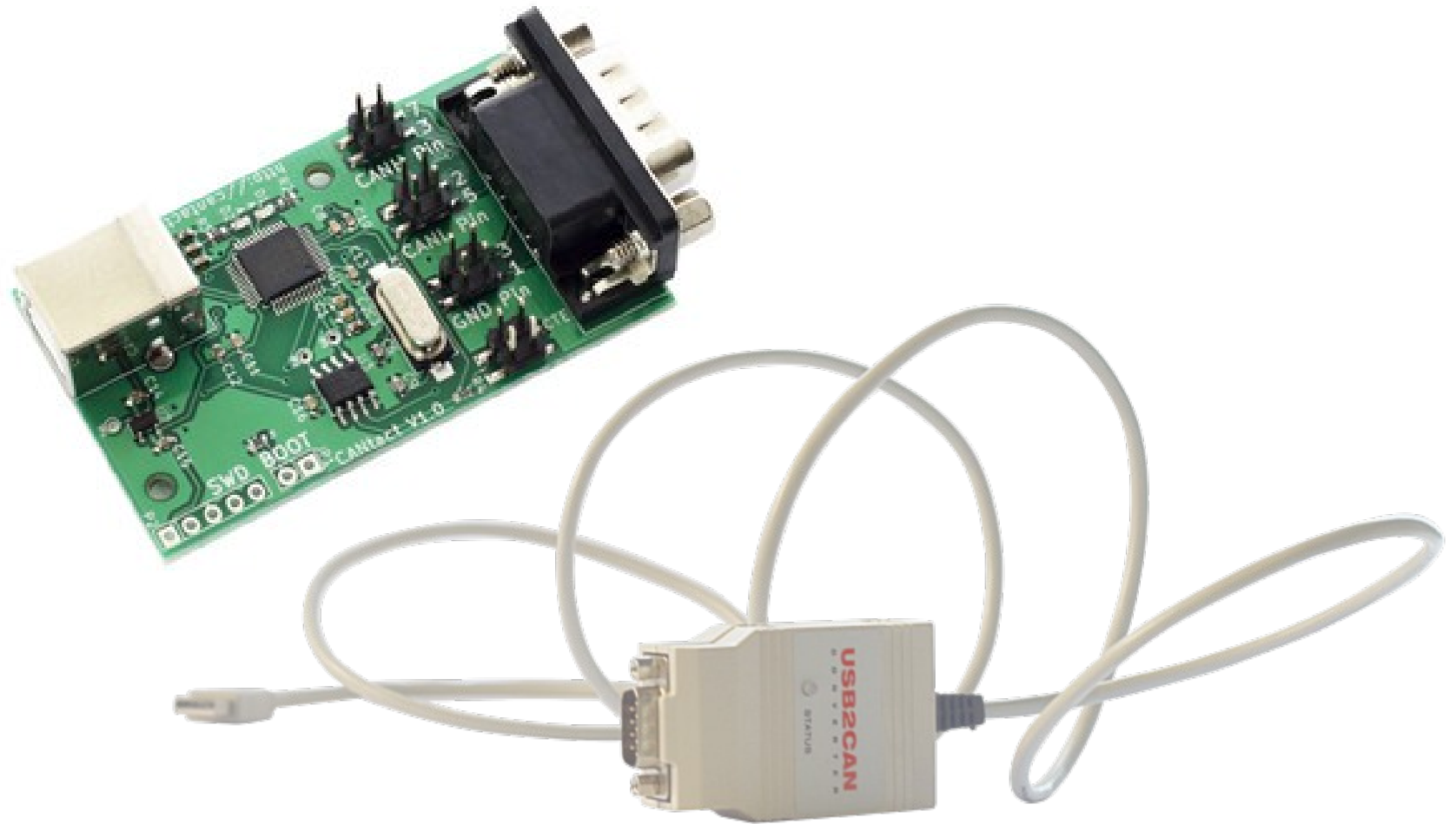


# Howto Build an Auto Brothel



# HW – CAN Bus (Cheap)



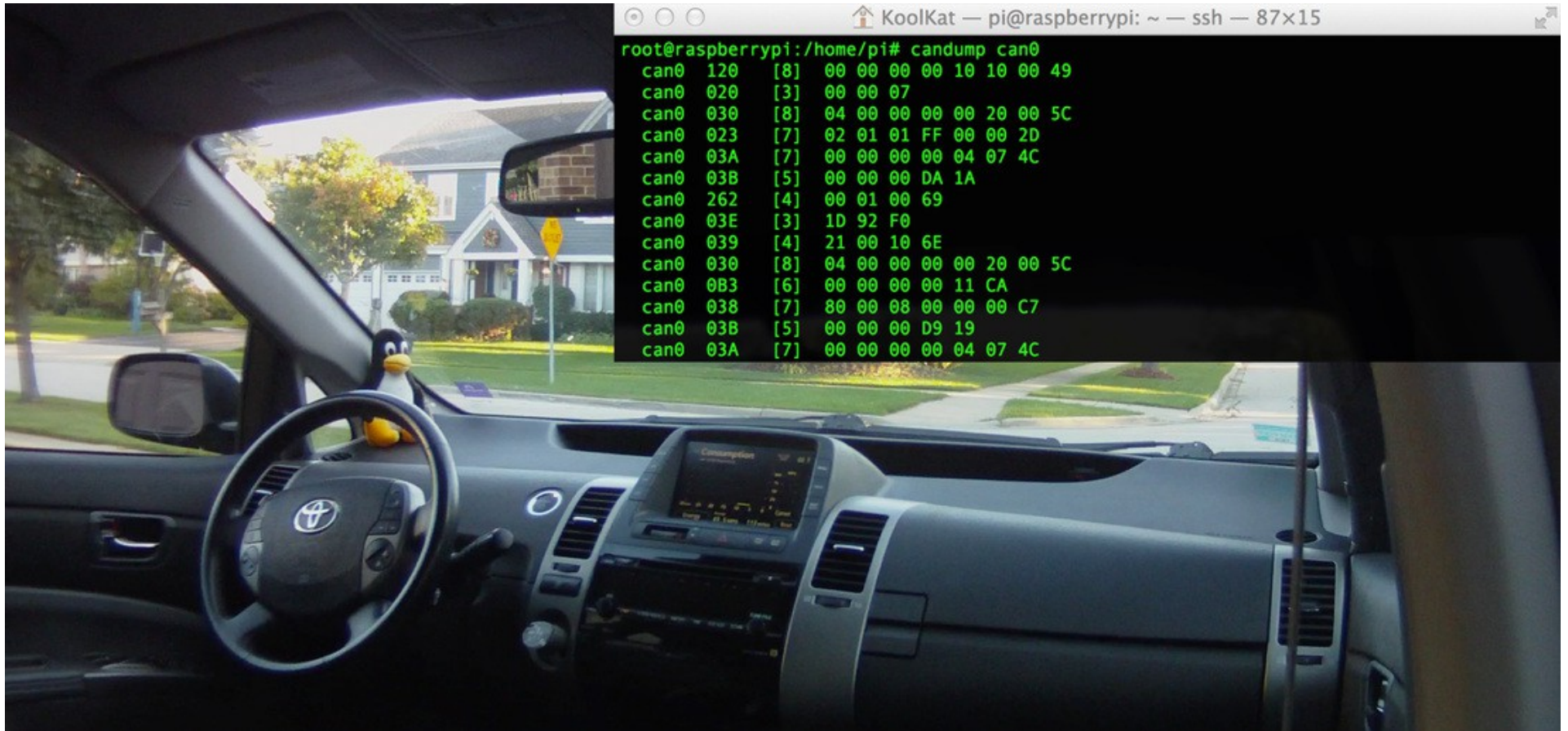
# HW - Scantools



# HW - Dealership Tools



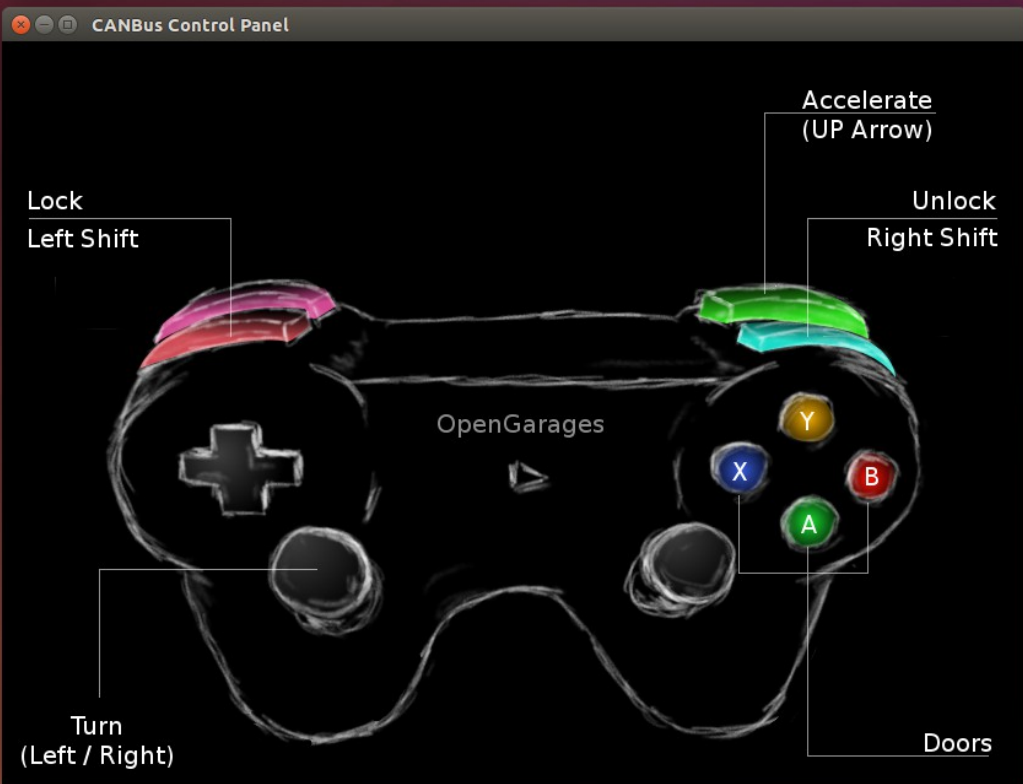
# SW - SocketCAN





# SW – ICSim (not new but...)

```
craig@nsa: ~/dev/git/ICSim
craig@nsa: ~/dev/git/ICSim x craig@nsa: ~/dev/git/ICSim x craig@nsa: ~/Documents/Te x
craig@nsa: ~/dev/git/ICSim 58x39
41 delta ID data ... < cansniffer vcan0
0.195294 39 00 0C ..
0.199606 95 80 00 07 F4 00 00 00 08 .....
0.199697 133 00 00 00 00 98 .....
0.199693 136 00 02 00 00 00 00 00 1B .....
0.200769 13A 00 00 00 00 00 00 00 19 .....
0.200774 13F 00 00 00 05 00 00 00 1F .....
0.199700 143 6B 6B 00 D1 kk..
0.200666 158 00 00 00 00 00 00 00 19 .....
0.200776 161 00 00 05 50 01 08 00 0D ...P.
0.199692 164 00 00 C0 1A A8 00 00 31 .....1
0.199609 166 D0 32 00 18 .2..
0.199696 17C 00 00 00 00 10 00 00 12 .....
0.199679 183 00 00 00 11 00 00 10 18 .....
0.506286 188 01 00 00 00 ....
0.199680 18E 00 00 5C ..\
0.200780 191 01 00 10 A1 41 00 38 ....A.8
0.199640 1A4 00 00 00 08 00 00 00 01 .....
0.200705 1AA 7F FF 00 00 00 00 68 01 .....h.
0.200716 1B0 00 0F 00 00 00 01 48 .....H
0.199590 1CF 80 05 00 00 00 00 2D .....-
0.199591 1DC 02 00 00 2A .....*
0.200557 21E 03 E8 37 45 22 06 3E ..7E".>
0.193468 244 00 00 00 33 13 ...3.
0.199482 294 04 0B 00 02 CF 5A 00 3B .....Z.;
0.210317 305 80 17 ..
0.200563 309 00 00 00 00 00 00 00 93 .....
0.199651 320 00 00 03 ...
0.199661 324 74 65 00 00 00 00 0E 0B te.....
0.199640 333 00 00 00 00 00 00 00 0F .....
0.200741 37C FD 00 FD 00 09 7F 00 0B .....
0.299539 405 00 00 04 00 00 00 00 29 .....)
0.299575 40C 00 00 00 00 04 00 00 13 .....
0.299542 428 01 04 00 00 52 1C 2F ....R./
0.300684 454 23 EF 18 #..
1.259754 5A1 96 00 00 00 00 00 62 10 .....b.
```



# 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)

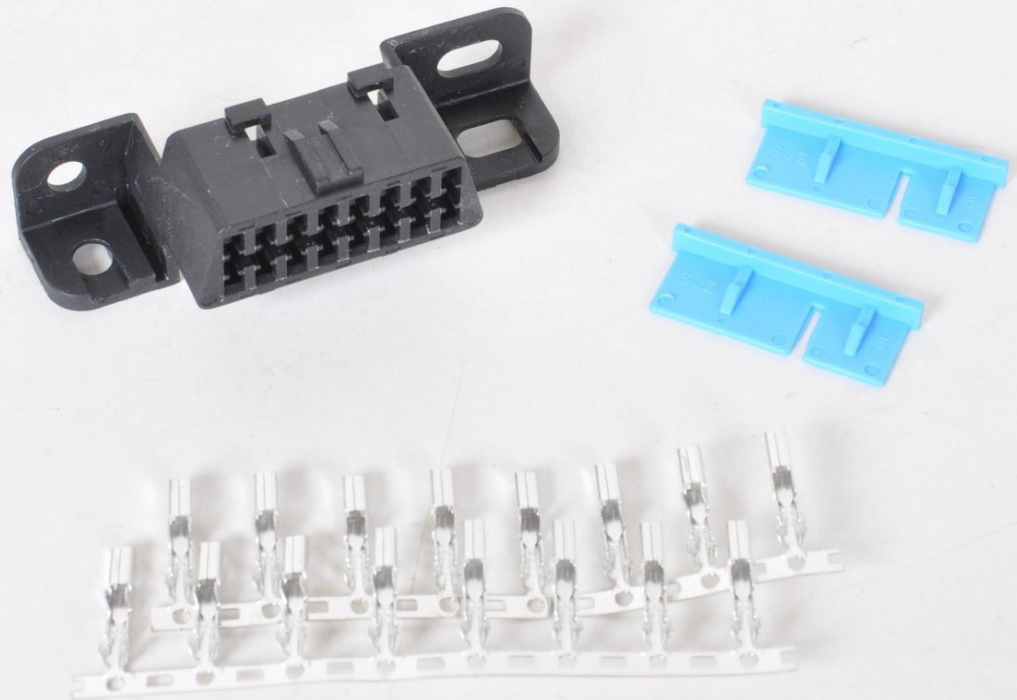
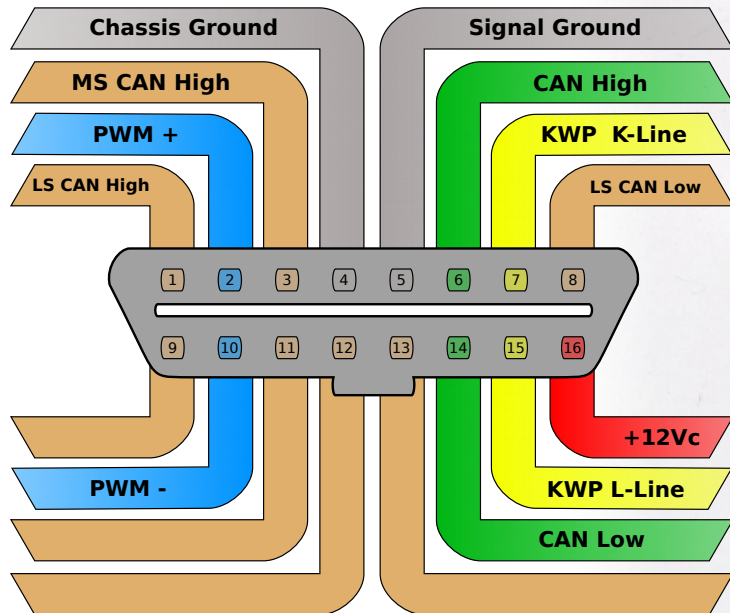
# Introducing ODB GW





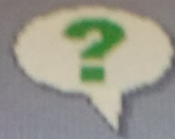
# Howto build your own ODB GW

- 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

VIN 2B3KA43R86H389824



2006 Dodge  
Charger  
2.7

Is this correct?

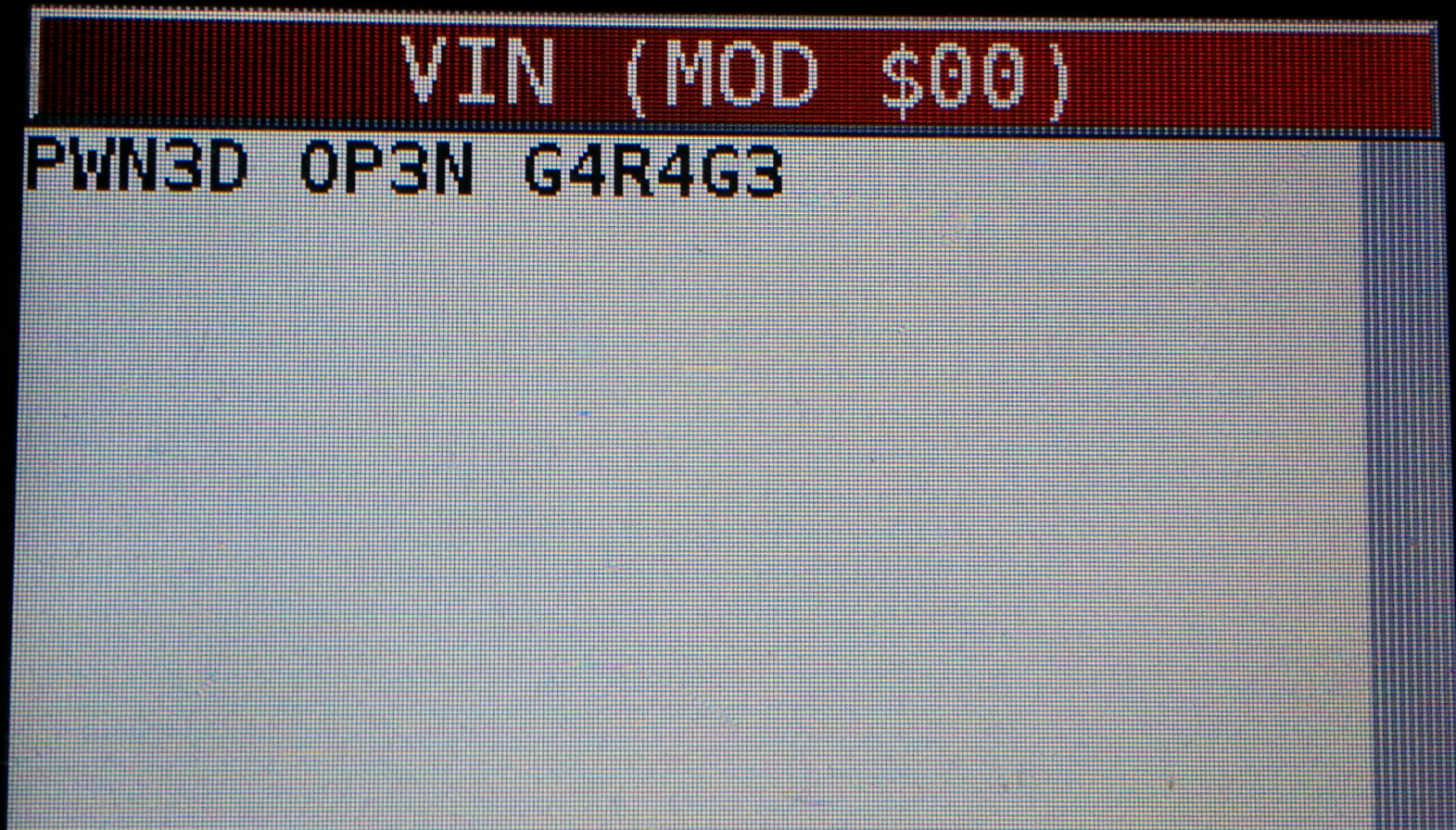
NO ←

YES ←



# 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

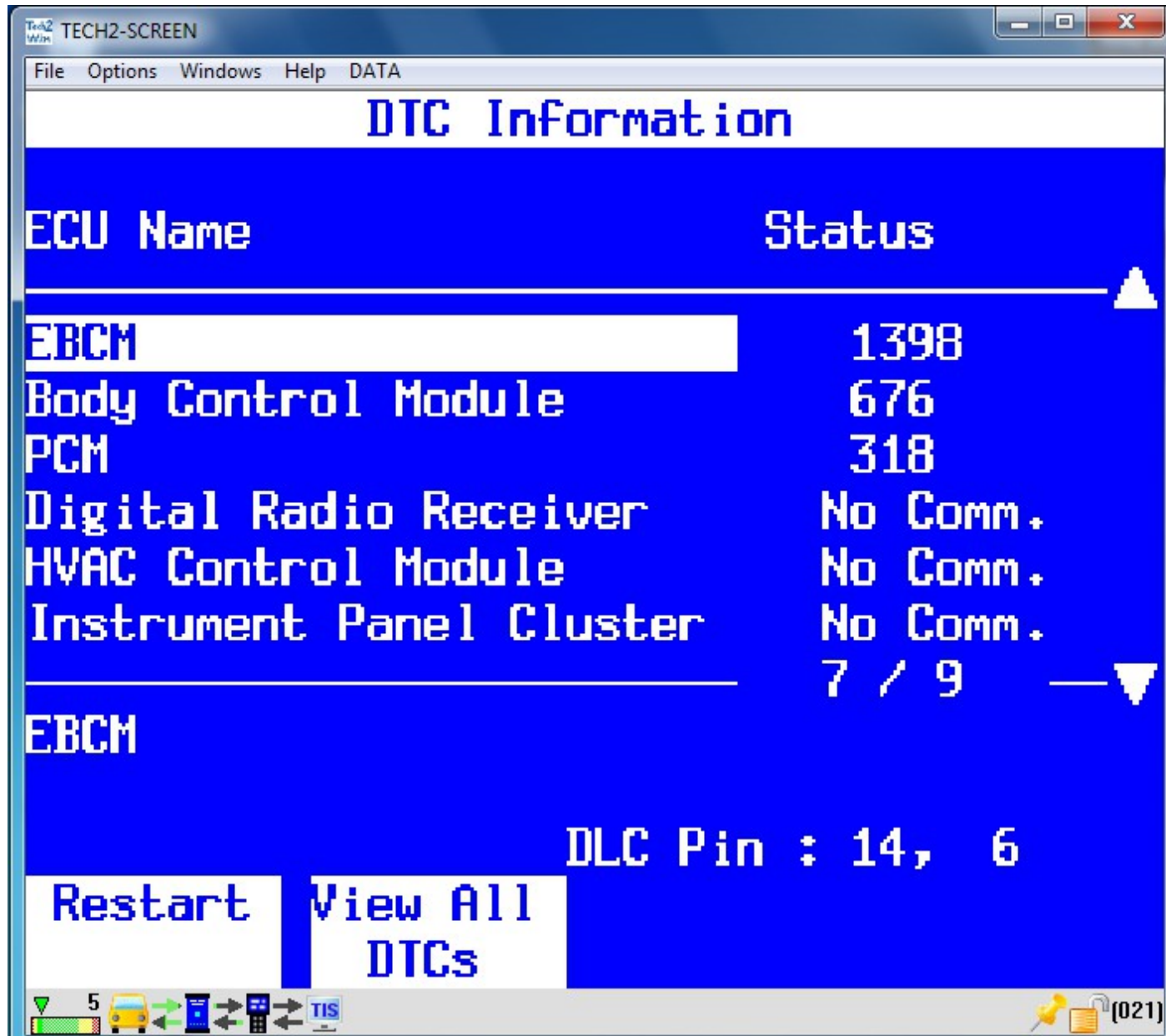
Received GM Read Data by ID Request

+ Stop Data Request





# Exploit all the trust



# Dealerships == squishy



# Vehicle STDs



How to participate

# Open Garages

