instructables

Food Living Outside Play Technology Workshop

Hack Your Car

by **Gadget Gangster** on May 31, 2012

Table of Contents

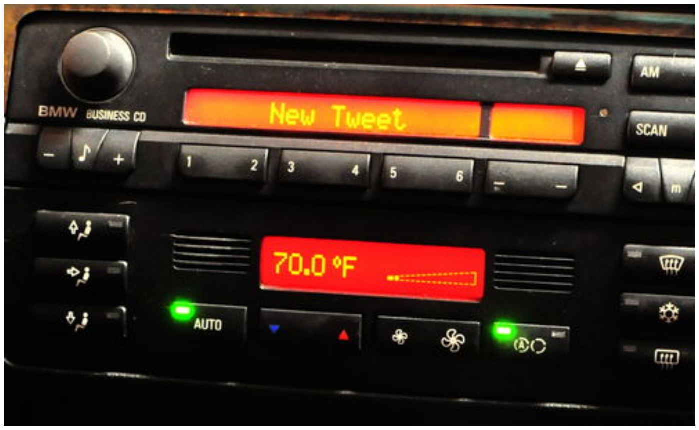
Intro: Hack Your Car

Want to unlock your car door with your phone? Re-map steering wheel buttons, or log performance data? The Car Kracker an open-source addon for your BMW 3-Series, 5-Series, 7-Series, X-Series or Mini that lets you;

- Add an Aux-In or music jukebox
- Remap steering wheel buttons
- Remove the Nav warning screen
- Display text like emails and SMS on your Sat Nav, radio, or dashboard
- Access engine and performance data like air/fuel ratio, oil pressure/temp, and VANOS
- Code retrofit parts like rain sensors, run-flat tires, theft alarms, and keys
- Access the proprietary error logs to troubleshoot engine, transmission, or accessory problems.

You can also upgrade Engine / Transmission firmware, remove the speed limiter, reset warning lights, and change dealer settings. Here's a little demo of displaying a tweet on the radio;

Continue to the next step and I'll answer a few questions, then I'll show you how to build your own.



Step 1: What is it?

Feautures

The Car Kracker is a microcontroller with a bit of hardware to talk to your car. It plugs into a connector in the trunk and has several default modes built-in;

- **Audio Jukebox Mode**: Play music stored on an SD card
- **Advanced Diagnostics Mode**: Remove the Nav warning screen, access error logs and read / modify ECU characteristics
- **Bus Sniffer**: Display data traffic and send test packets
- **Audio Aux-In Mode**: Enable Aux input to stereo headunits

A kit is available , or you can follow the schematic in the next step to make one from scratch. Everything is open source, so it be customized and the firmware can be updated via USB. A few ideas;

- Traffic Camera Alerter
- Automatic Audio sync
- Auto Unlock: Unlock the doors when a specific Bluetooth device comes within range
- Data logger + phone home: Automatically send car location and speed via SMS

Will it work with my car?

The Car Kracker works with the following cars;

- BMW
  - 3-Series, 1998 - 2007 (e46)
  - 5-Series, 1995 - 2004 (e39)
  - 7-Series, 1994 - 2001 (e38)
  - X3, 2004 - 2010 (e83)
  - X5, 1999 - 2006 (e53)
  - Z4, 2002 - 2008 (e85, e86)
- Mini
  - One / Cooper / S, 2001 - 2006 (r50, r53)
  - Convertible, 2005-2008 (r52)
- Land Rover
  - Range Rover, 1999 - 2003 (L30)

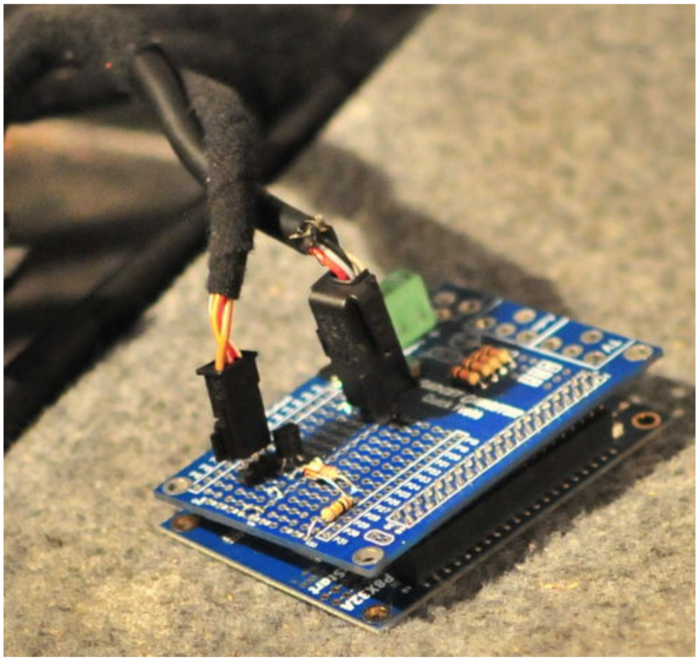
Will it break my car?

Unless you want to update the firmware on your Engine / Transmission, It's pretty much impossible - the data bus is designed so that errant / malfunctioning devices don't break anything. Changing preferences (like turning off the door gong) just updates the settings memory, the firmware doesn't change.

Credits

The Car Kracker builds on many people's work - Many thanks to Dr_Acula for respinning RS232, Jochen @ Navcoder, the BMWCoders forums, Rayman for audio playback, e46fanatics, and bimmerforums. Thanks Everybody!

Continue on and I'll show you how to make your own!



Step 2: Make it: Parts

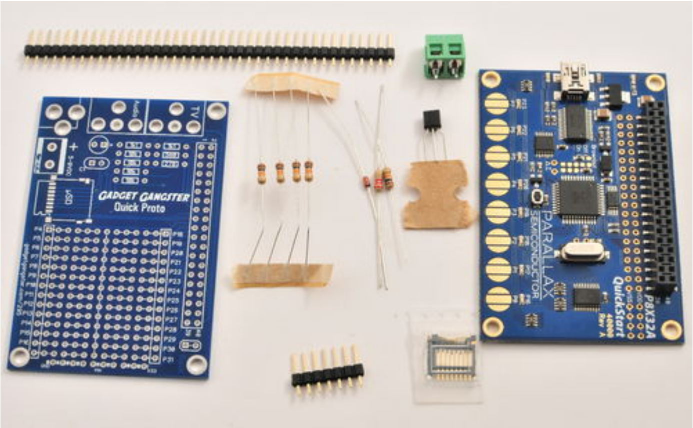
Below are the parts you'll need to build your own Car Kracker - We also offer a kit that includes everything you need right here . The kit also comes pre-programmed and includes a USB cable and mounting hardware.

Parts List

- P8X32A + Quick Proto
- Qty 47: Pin headers
- Resistors;
  - 1x 22k ohm, 1/4 Watt Resistor
  - 5x 10k ohm, 1/4 Watt Resistors
- Diodes;
  - 1x 1n4148 Diode
  - 1x 2n3904 BJT Transistor
- SD Card slot (Hirose DM-3D-SF)

The kit comes pre-programmed, but if you're building it yourself, you can grab the sourcecode right here . Here's the circuit we're going to build;

Check to make sure you have everything you need, warm up your soldering iron, and continue to the next step



Step 3: Make it: Assembly

Let's start by adding the 10k Resistors, they're marked with Brown - Black - Orange stripes and the 22k resistor;

Save the extra leads as you trim them off each resistor.

The diode and transistor - note the black stripe on one side of the diode. That side points down, as shown in the photo. The flat side of the transistor points down, too;

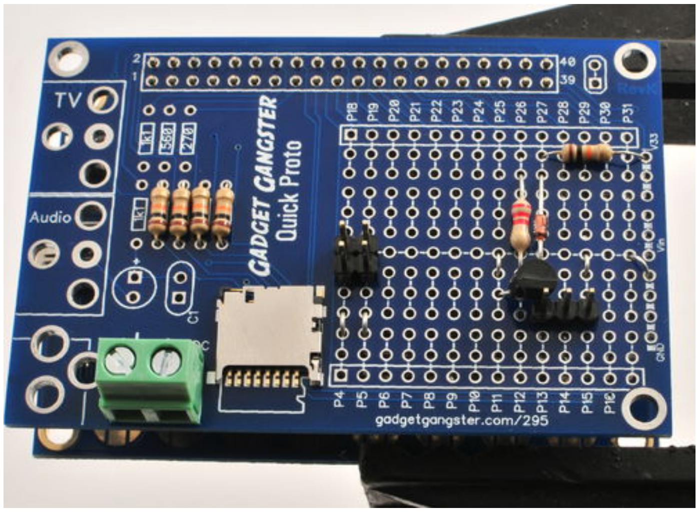
Using the extra wire from the resistors, add 5 jumpers to the board, I've marked them in the photo

Add the audio and bus connectors;

Now the microSD card slot - note that you don't have to add this unless you want the audio jukebox features.

Now the power connector and finally the header. It's easiest to first insert the header pins into the P8X32A board, then put your Quick Proto board on top

Assembly's all done. Let's test it out!


TV
Audio
GADGET GANGSTER
Quick Proto
P18 P19 P20 P21 P22 P23 P24 P25 P26 P27 P28 P29 P30 P31
P4 P5 P6 P7 P8 P9 P10 P11 P12 P13 P14 P15 P16
gadgetgangster.com/295

Step 4: Connect to your Car

First, let's locate the data bus on your car;

1 - The Trunk
Even if your car didn't come with a CD changer, it's nearly always pre-wired for it. Open up your trunk and explore behind the felt panel on the driver's side. You'll find three cables - The 3 pin cable is your bus connection, and the 6 pin cable is the analog audio input to your stereo. You don't need the big 20 pin connector.

Plug the 3 pin and 6 pin cables into your Car Kracker;

2 - OBD2 Connector
The Trunk connection lets you access all the accessories in the car, but not the Engine Control Unit or Transmission Control Unit. To access the engine and transmission, you'll need to connect through the 'On Board Diagnostics' connector. It's in the car under the steering wheel, and looks like this;

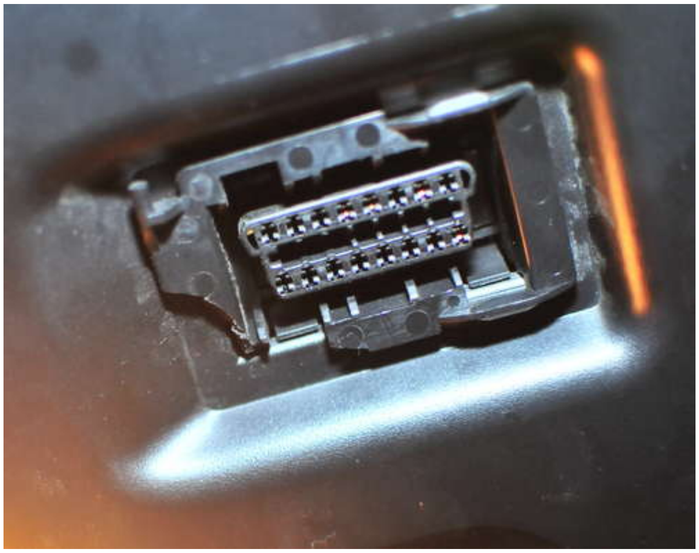
Use a bit of jumper wire to connect each pin of the Car Kracker to these OBD pins;

The leftmost pin on the Car Kracker connects to pin 7 and pin 8 on the OBC port. The middle pin doesn't get connected. The rightmost pin gets connected to pin 5.

3 - Diagnostic Connector
Some cars will also have a diagnostic connector under the hood - mine has a huge connector which includes bus connections, and a couple other random things (like two connectors to reset the oil change reminder);

For the BMW 'Pacman' connector, connect the two data lines to the leftmost pin on your Car Kracker, and the Ground port to the rightmost pin.

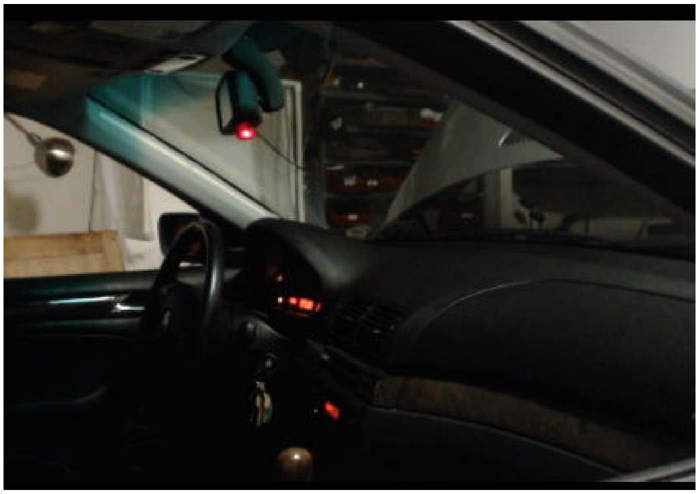
When doing diagnostics, I usually use the Pacman connector - for audio and entertainment, I use the trunk connector.



Step 5: Using it: Connection Test

Let's start by doing the connection test; power up your Car Kracker and hold the button labelled P4. That will start the connection test and blink the 'Clown Nose' light on the mirror on and off. Here's what it looks like;

Now that you're connected, let's start using it!



Step 6: Using it: Audio Aux-In

If you boot up the Car Kracker without holding a button and without an SD card, you'll enter Audio Aux-In mode. This mode lets you connect any MP3 player or even bluetooth player and listen to it on your stereo. Here's how to set it up;

Aux-In

The 6-pin header in the trunk connects to an analog audio input to your stereo. Unfortunately, the stereo won't tune into that audio input unless it thinks there's a CD changer connected in your car.

The Car Kracker solves that problem by pretending to be a CD changer. Your stereo will think there's a CD changer and amplify whatever signal is coming in the analog in line. Here's how to set it up;

Step 1: CD Changer Emulation
With the Car Kracker connected to your car, turn it on without inserting an SD card. After a few moments, it will be CD changer emulation mode. Whatever audio signals come in through the CD changer audio connection will be played on your stereo.

Step 2: Headphone Jack Connection
You can connect whatever audio source directly to the 6-pin header in the trunk, although that can be inconvenient. You can use a Bluetooth A2DP adapter and play audio from your cell phone over bluetooth, or you can connect your audio source directly to your stereo. On the BMW 3-Series, you just pry off the fake wood panels on the dash with a butter knife. First the passenger side panel, then the middle panel;

and remove the two screws holding in the stereo;

Remove the connectors off the back and slide out the stereo;

You'll want to connect your left channel, right channel, and ground to the pins on the bottom;

You can run that cable out to the sunglasses box under the stereo or to the glove box.

A few notes on Aux-In;

- Your Car Kracker has to be powered up and connected to the car whenever you want to use Aux-input. You can power it up with 4xAA's batteries or connect it to a USB car charger.
- Not all head units need CD changer emulation - some have a second set of audio connectors just for Aux-input. In that case, you just need to construct a cable.

Step 7: Using it: Audio Jukebox

If you want to keep everything in the trunk, the Car Kracker can play back audio files stored on the SD card. Just boot up the Car Kracker with an SD card connected and it will enter Audio Jukebox mode. Here's how to use it;

Jukebox Mode

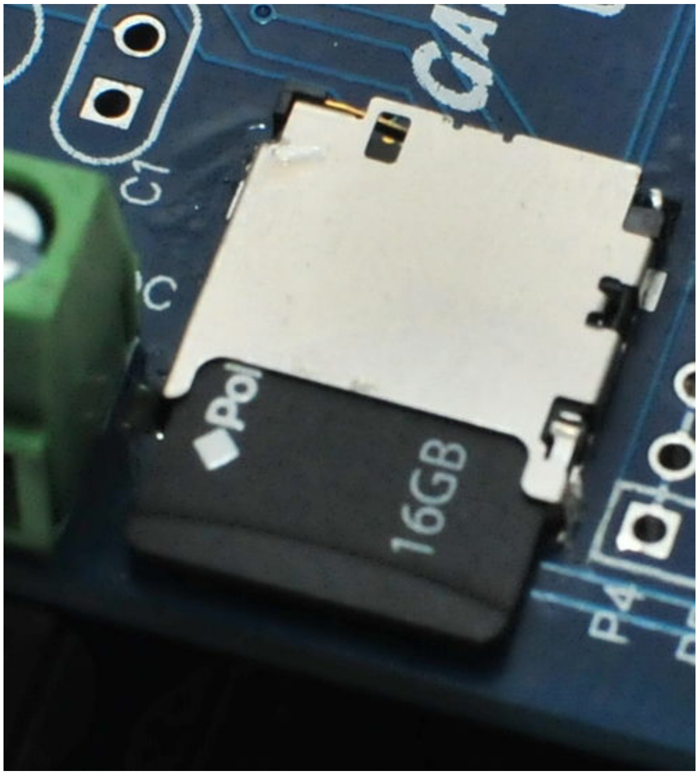
Step 1: Pick your tunes
The Car Kracker plays back 44khz and 48khz stereo wav files so your MP3's and AAC's will need to be converted. I use Audacity for this - conversion takes just a few minutes.

Step 2: Load 'em up
SD cards up to 32GB are supported, copy your songs over to the SD card, cards up to 32GB are supported. You can use the buttons on your radio to move between albums and tracks - Albums are grouped by filename, your SD card should look something like this;

- 01_01.wav
- 01_02.wav
- 01_03.wav
- 02_01.wav
- 02_02.wav
- and so on...

Put everything on the root of the card, no need to use directories.

Step 3: Listen!
Hit 'CD' on your radio - the first selection will change to the built-in CD player. The second time you hit 'CD', it will switch to our virtual CD changer. The CD1 and CD2 buttons change between albums, and the left and right arrows change between tracks



Step 8: Using it: Advanced Diagnostics

If you want to troubleshoot a slipping transmission, an A/C that never gets cold, or a Check Engine light, your Car Kracker can do just about everything. Here's a walkthrough;

Setting it up takes two steps;

1 - Connect to your car
Connect your Car Kracker to your car and hold down the P6 button on boot up to enter diagnostics mode. To do diagnostics on the engine / transmission, you'll need to connect to the OBD / diagnostic connector instead of the Trunk connection.

2 - Setup the software
The Car Kracker is going to provide a physical connection between your car and computer. You're going to run software on your computer to actually collect the diagnostic data. You have a few choices;

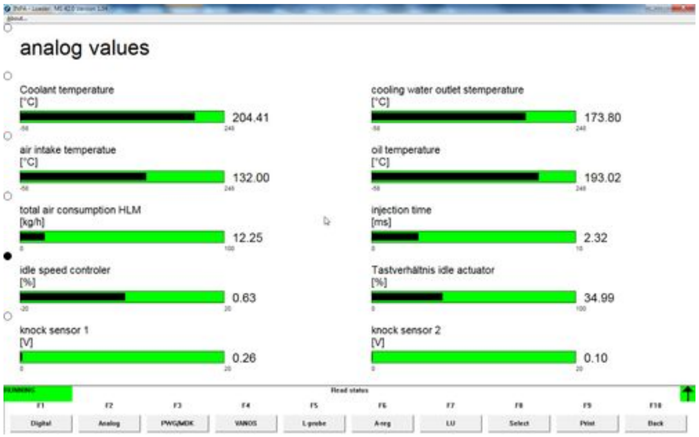
INPA
INPA is not commercial software, it can be found on 'the usual sources'. I suspect it was originally for BMW re-certification and factory testing. Downloads usually include NCSExpert, WinkFP, and a few other tools.

INPA comes with EDIABAS, which needs to be configured. In c:\EDIABAS\BIN\EDIABAS.ini, make sure active interface is Interface =STD:OBD . Also, your Car Hacker needs to be assigned to COM1.

With INPA installed, start INPA(_.IPO). That will load EDIABAS and INPA will pop up. Select the type of car you have and the diagnostics you want to run and you're off to the races!

NAVCODER
Navcoder is commercial software, it is mostly designed to read accessory bus information (Radio / lights / Nav), not really for engine diagnostics. However, it's pretty handy and easy to use, especially when you want to do things like remove the Nav warning screen or change the speed sensitive volume on the stereo;

The free version did everything I needed it to do, but I ended up buying it just to say thanks.


analog values

Coolant temperature [°C] 204.41

cooling water outlet stemperature [°C] 173.80

air intake temperatue [°C] 132.00

oil temperature [°C] 193.02

total air consumption HLM [kg/h] 12.25

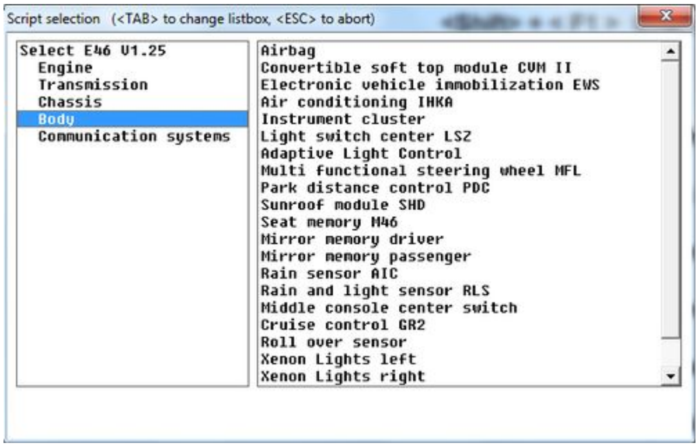
injection time [ms] 2.32

idle speed controler [%] 0.63

Tastverhältnis idle actuator [%] 34.99

knock sensor 1 [V] 0.26

knock sensor 2 [V] 0.10


Script selection (<TAB> to change listbox, <ESC> to abort)

```
Select E46 V1.25         Airbag
  Engine                 Convertible soft top module CVM II
  Transmission           Electronic vehicle immobilization EWS
  Chassis                Air conditioning IHKA
  Body                   Instrument cluster
  Communication systems  Light switch center LSZ
                         Adaptive Light Control
                         Multi functional steering wheel MFL
                         Park distance control PDC
                         Sunroof module SHD
                         Seat memory M46
                         Mirror memory driver
                         Mirror memory passenger
                         Rain sensor AIC
                         Rain and light sensor RLS
                         Middle console center switch
                         Cruise control GR2
                         Roll over sensor
                         Xenon Lights left
                         Xenon Lights right
```

Step 9: Using it: Dealer Customizations

You can put the Car Kracker in diagnostics mode (Hold P7 on bootup) to make customizations to your car;

What are customizations?
Customizations are ways to control the default behaviors of the electronics in the car. For instance;

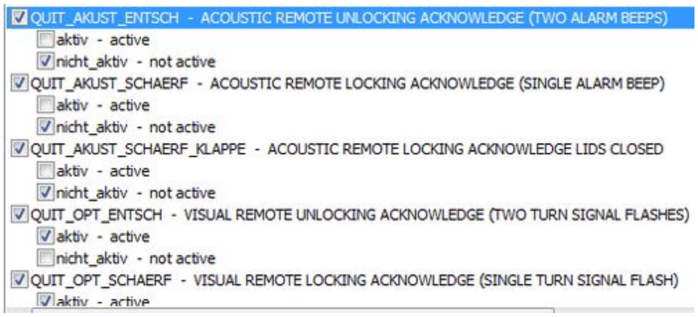
- Should the nav warning screen be displayed?
- Should the gong sound be played whenever the door is open?
- Should there always be daylight running lights?

And so on. Only some things can be customized, it depends on the functionality of each module. Customizations are stored even when the battery is disconnected, but they can be changed any number of times. Personally, I turned off the 'Keys in ignition' gong and reduced the level of the speed sensitive steering. Here's how to customize your car;

1 - Make sure INPA works
Also make sure you've installed NCSExpert, it usually comes with INPA.

2 - Use NCSExpert to change customizations
A full writeup on NCSExpert is up on M3 Cutters . I also use NCSDummy (on Bimmerforums) because NCSExpert is entirely in German and can be hard to understand.

NCSExpert will generate a file (usually C:\NCSEXPER\WORK\NETTODAT.TRC), open NCSDummy and it will load that file and allow you to edit it easily. Save the edit and write the revised file back to your car with NCSExpert.


☑ QUIT_AKUST_ENTSCH - ACOUSTIC REMOTE UNLOCKING ACKNOWLEDGE (TWO ALARM BEEPS)
  □ aktiv - active
  ☑ nicht_aktiv - not active
☑ QUIT_AKUST_SCHAERF - ACOUSTIC REMOTE LOCKING ACKNOWLEDGE (SINGLE ALARM BEEP)
  □ aktiv - active
  ☑ nicht_aktiv - not active
☑ QUIT_AKUST_SCHAERF_KLAPPE - ACOUSTIC REMOTE LOCKING ACKNOWLEDGE LIDS CLOSED
  □ aktiv - active
  ☑ nicht_aktiv - not active
☑ QUIT_OPT_ENTSCH - VISUAL REMOTE UNLOCKING ACKNOWLEDGE (TWO TURN SIGNAL FLASHES)
  ☑ aktiv - active
  □ nicht_aktiv - not active
☑ QUIT_OPT_SCHAERF - VISUAL REMOTE LOCKING ACKNOWLEDGE (SINGLE TURN SIGNAL FLASH)
  ☑ aktiv - active

Step 10: Using it: Bus Sniffing

If you're an advanced user and just want to watch the data bus to see what's going on, hold down P7 on boot up to enter Bus Sniff mode. This will show you the traffic on the databus in realtime;

Once you enter Bus Sniff mode, open up your Serial terminal program (Hyperterm, PuTTY, Parallax Serial Terminal) and connect to the COM port your Car Kracker is on at 115200 baud.

- The first byte of the message is the source; $00 = broadcast, $3B = Nav, $BF = Global
- The second byte is the length of the message, counting from the third byte
- The third byte is the destination - the mapping is the same as the source addresses
- The 4th byte begins the data itself.
- The last byte is the checksum - it's calculated by XOR'ing each byte in the packet, here's the pseudo code;
  ```
  checksum := 0
  Repeat i from 0 to codelength
  checksum := checksum xor (BYTE[code][i])
  ```

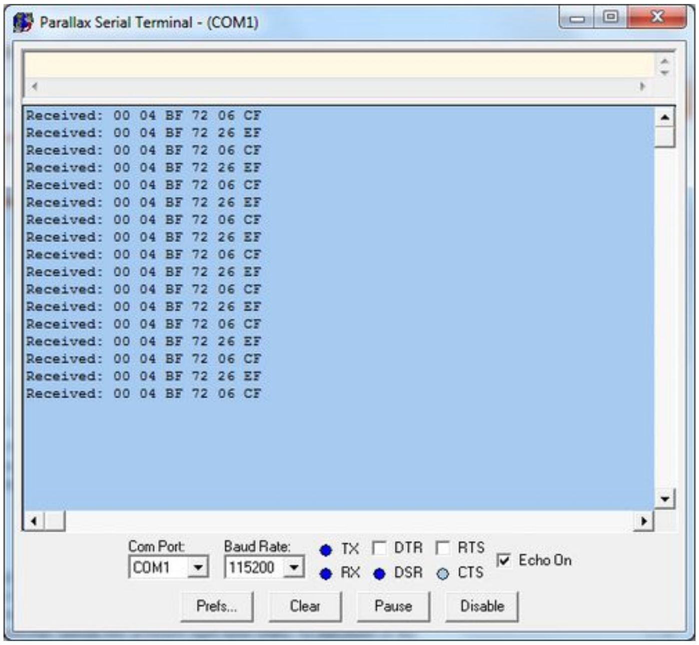
There is no discovery method for finding out what commands each module supports. The best way to figure it out is watch the bus while pushing buttons. The example above is what the bus does when I unlock the door with the key fob;

$00 $04 $BF $72 $06
From: Broadcast ($00) To: Global ($BF)
Data: $72 $06

Remote Unlock button pressed on Key fob

$00 $04 $BF $72 $26
From: Broadcast ($00) To: Global ($BF)
Data: $72 $26
Remote Unlock button released

Let's talk about customizing your Car Kracker to do all kinds of crazy stuff.



Parallax Serial Terminal - (COM1)

```
Received: 00 04 BF 72 06 CF
Received: 00 04 BF 72 26 EF
Received: 00 04 BF 72 06 CF
Received: 00 04 BF 72 26 EF
Received: 00 04 BF 72 06 CF
Received: 00 04 BF 72 26 EF
Received: 00 04 BF 72 06 CF
Received: 00 04 BF 72 26 EF
Received: 00 04 BF 72 06 CF
Received: 00 04 BF 72 26 EF
Received: 00 04 BF 72 06 CF
Received: 00 04 BF 72 26 EF
Received: 00 04 BF 72 06 CF
Received: 00 04 BF 72 26 EF
Received: 00 04 BF 72 06 CF
Received: 00 04 BF 72 26 EF
Received: 00 04 BF 72 06 CF
```

Com Port: COM1
Baud Rate: 115200
● TX □ DTR □ RTS
● RX ● DSR ○ CTS
☑ Echo On

Step 11: Using it: Advanced Hacking

The Car Kracker was written to be reused! If you ever done a little programing, you can customize it to do all kinds of things. First, download the code and install the Propeller Tool (download). Open up 'KMB_Kracker_Demo.spin' and this is what you'll see;

This little program does two things; it helps you find your car in a crowded parking lot by blinking the clown nose when you hit unlock on your keys. It also remaps the R/T button on your steering wheel to pop open your trunk.

First, we start up the Kbus driver with Kbus.start(27,26), then we enter a loop. The loop first waits for an incoming kbus code. If the code matches 'remote home button pushed', it sends the 'Blink the Clown nose' code. If it sees the RTbutton has been pushed, it sends a 'TrunkOpen' Code.

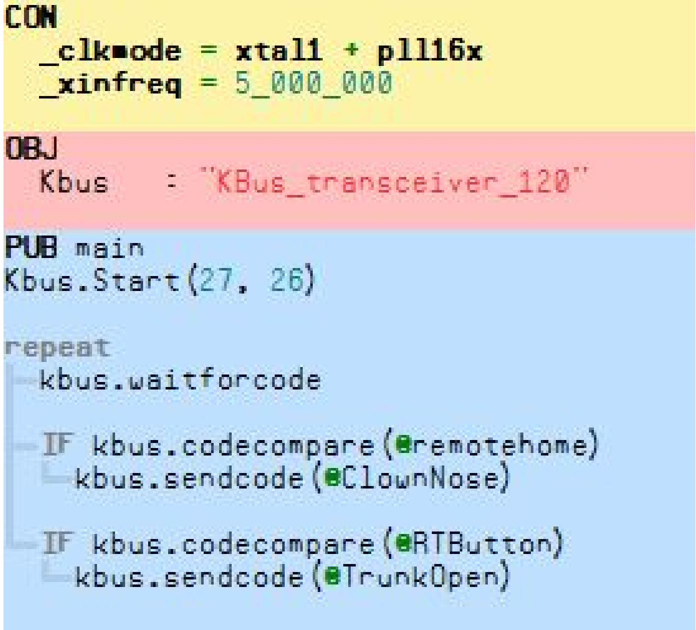
Other functions available include;

`kbus.sendtext(@textptr)`
Send text stored at the location given to the radio text display

`kbus.textscroll(textptr)`
Send text stored at the location give to the radio. Scroll it if too long

`kbus.checkforcode(time)`
Wait for time (given in milliseconds) for an incoming code. Return -1 if no code was received. Return 1 if a code was received. The received code can then be compared using kbus.codecompare

`kbus.waitforcode`
Wait until an incoming code is received. The received code can then be compared using kbus.codecompare.



```
CON
  _clkmode = xtal1 + pll16x
  _xinfreq = 5_000_000

OBJ
  Kbus    : "KBus_transceiver_120"

PUB main
Kbus.Start(27, 26)

repeat
  kbus.waitforcode

  IF kbus.codecompare(@remotehome)
    kbus.sendcode(@ClownNose)

  IF kbus.codecompare(@RTButton)
    kbus.sendcode(@TrunkOpen)
```