Car Hacking: For Poories

Dr. Charlie Miller (@0xcharlie)

Chris Valasek (@nudehaberdasher)

Introduction

Who

- **Charlie Miller**
  [Security Engineer]
  |**Twitter**|

- **Chris Valasek**
  [Director of Security Intelligence]
  |**IOActive**|

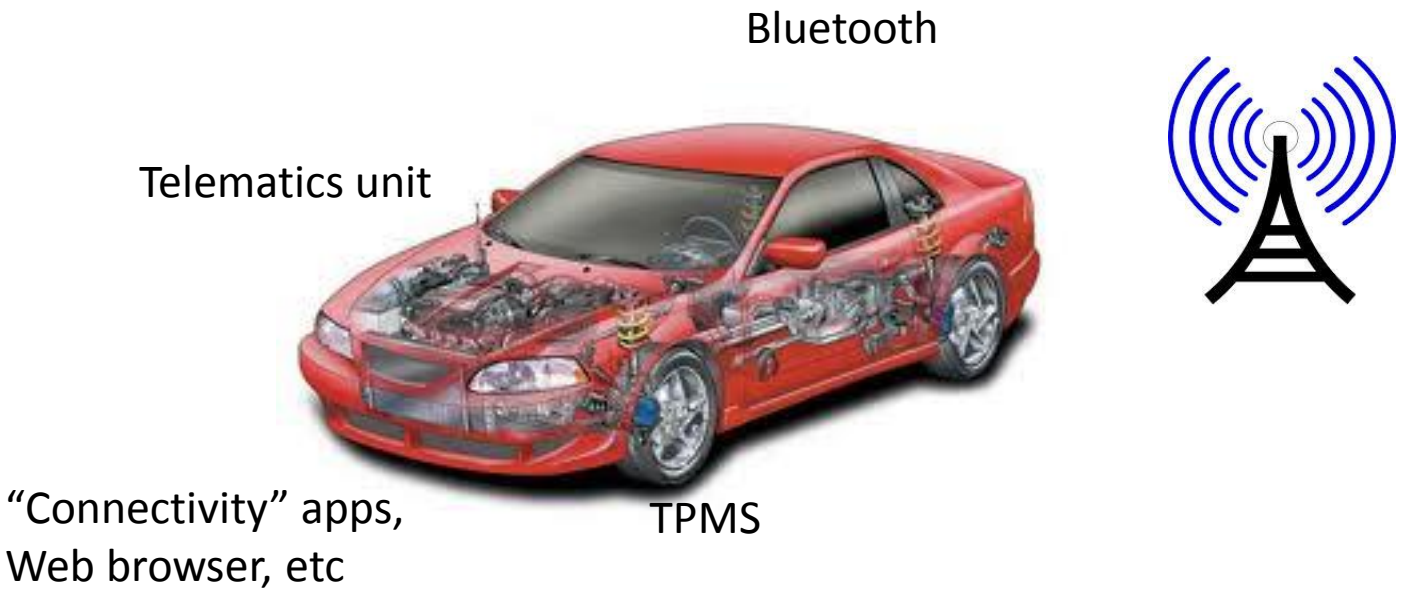
Agenda

- Anatomy of an attack
- Why this research is hard
- Car hardware for software people
- The Workbench
- The Mobile Platform

Anatomy of an Attack

Step 1: Code execution

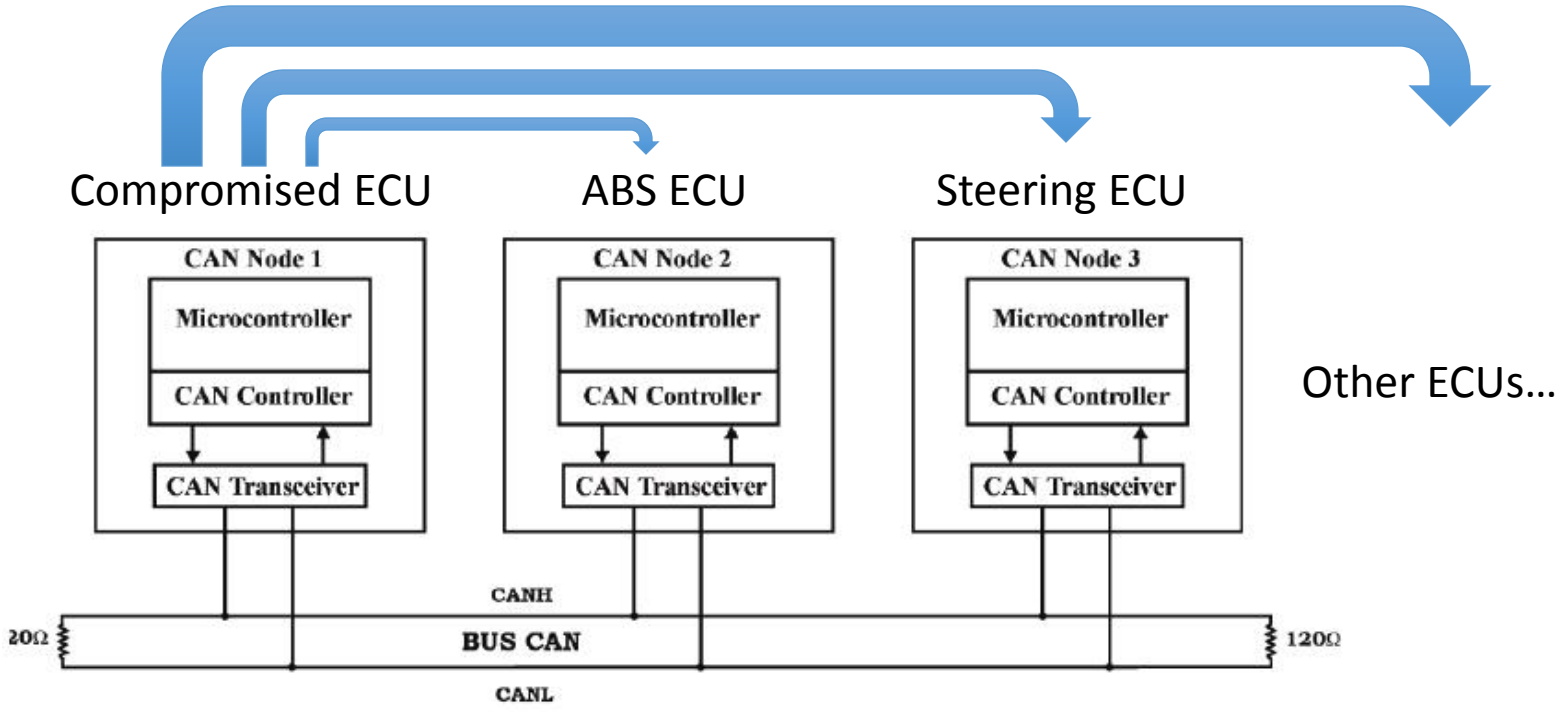
- Remote



Step 1: Code execution (cont.)

- Local

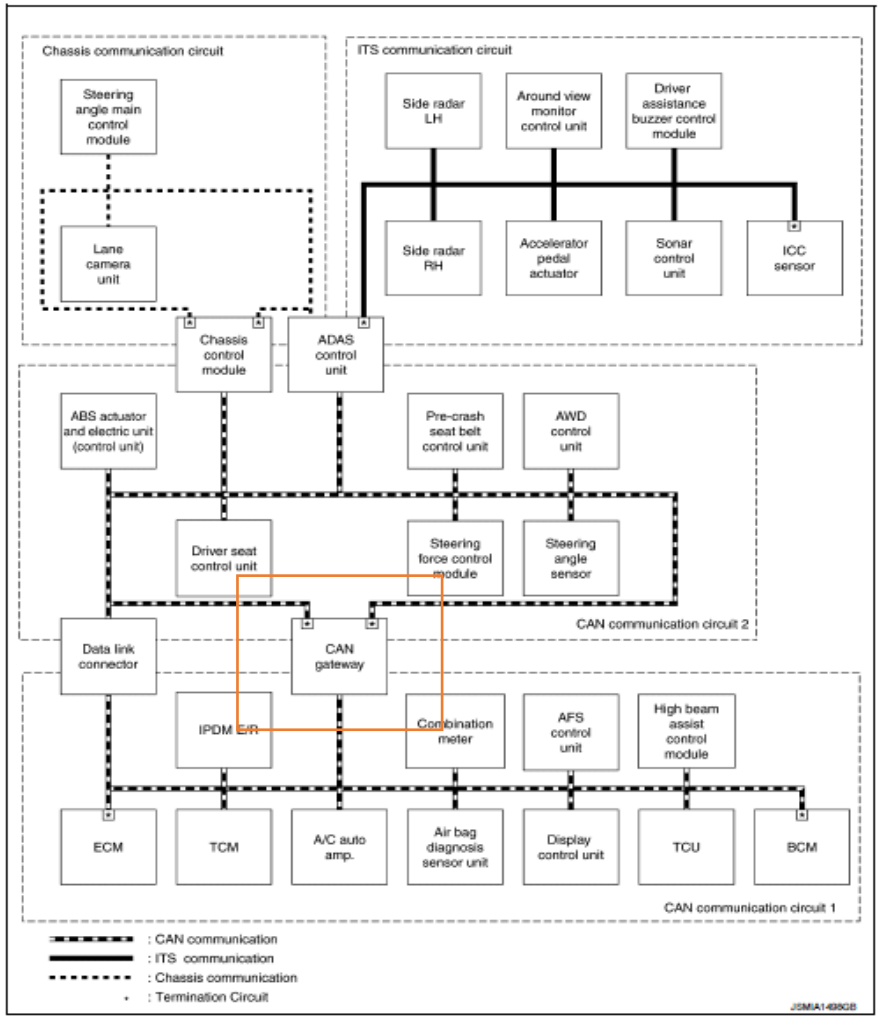
Step 2: CAN message injection



Step 2.5: Gateway bypass/reprogramming

< SYSTEM DESCRIPTION > [CAN]

With ICC



Attacks

- Steering
- Braking
- Acceleration
- Microphone
- Display

Car Hacking is Hard

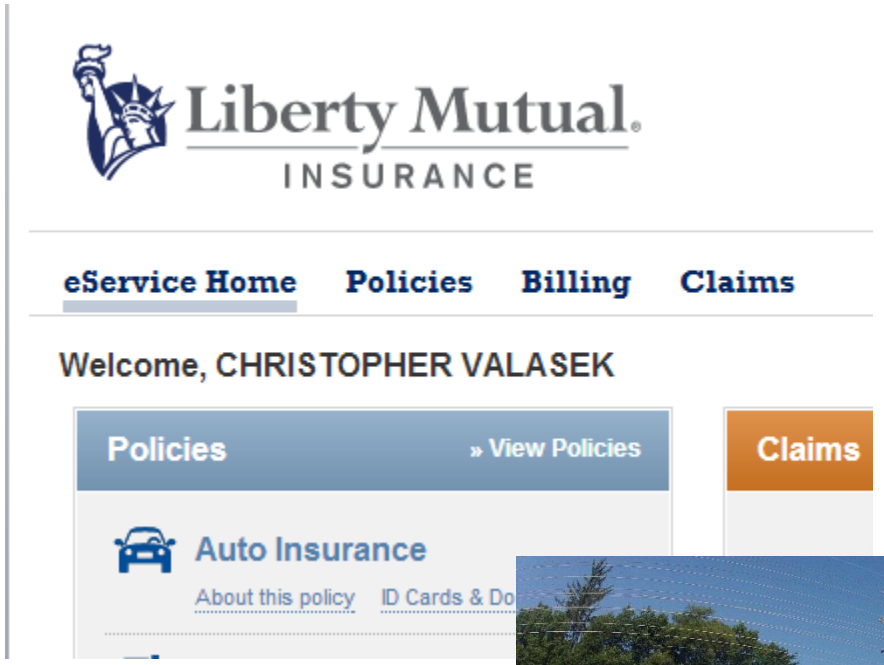
Expensive: Ford

Cash Price of Vehicle & Accessories	$
STATE AND LOCAL TAXES (If any)	19410.00
Documentary Fee	1358.00
License, License Transfer, Title, Registration Fee	129.00
	~~68.50~~
TOTAL PRICE OF UNIT	$ 20965.50
TOTAL CREDIT (TRANSFERRED FROM LEFT COLUMN)	$ ~~N/A~~
UNPAID CASH BALANCE DUE ON DELIVERY	$ 20965.50

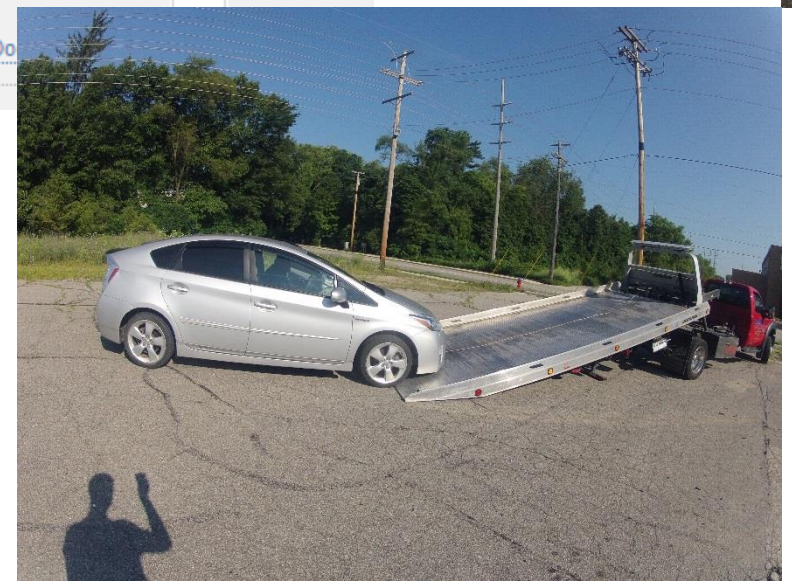
Expensive: Toyota

Cash Price of Vehicle & Accessories	$	29310.00
STATE AND LOCAL TAXES (If any)		2051.00
Documentary Fee		129.00
License, License Transfer, Title, Registration Fee		68.50
TOTAL PRICE OF UNIT	$	31558.50
TOTAL CREDIT (TRANSFERRED FROM LEFT COLUMN)	$	N/A
UNPAID CASH BALANCE DUE ON DELIVERY	$	31558.50

Other costs


Liberty Mutual
INSURANCE
eService Home
Policies
Billing
Claims
Welcome, CHRISTOPHER VALASEK
Policies
» View Policies
Claims
Auto Insurance
About this policy
ID Cards & Do


PRIUS
PENNSYLVANIA
HXL•8875



Cost of research

$0 $5,000 $10,000 $20,000 $40,000

Can we get the cost
of car hacking research
down here?

Car Hacking, for the poors

‘What, the poories want free healthcare? Shut it all down’ – Jesus Christ

Lower the cost!

- Cars are expensive
  - Used/New ECUs are not in comparison
- Isolated ECUs can be used to identify CAN IDs and application data
- Error and legitimate data can be identified by adding/removing connections
- Develop a mobile platform for testing requiring movement
  - Brakes, Steering, Intelligent Transportation System

Hardware is hard

(for software people)

Before you begin…

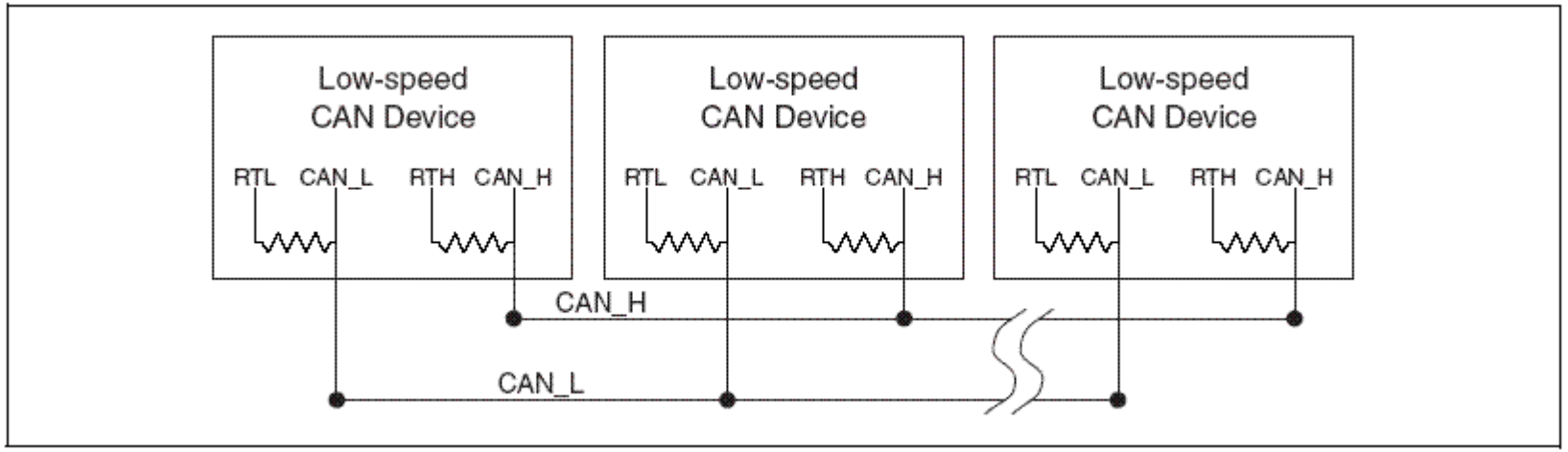
- Basic electronics
  - Grounds, power, multimeter, soldering, twisting wires together, duct tape
- CAN Architecture / topology
  - How ECUs are connected, interact, and CAN Gateways
- General wiring diagrams, specifically for cars
  - This will save you hours of time. It took us a while to trust the diagrams, because we're software idiots
- Automotive disassembly
  - Instructions or crowbar+hammer
- Patience
  - Everything takes way longer if you're not mechanics / very familiar with cars

CAN Basics

Physical Edition

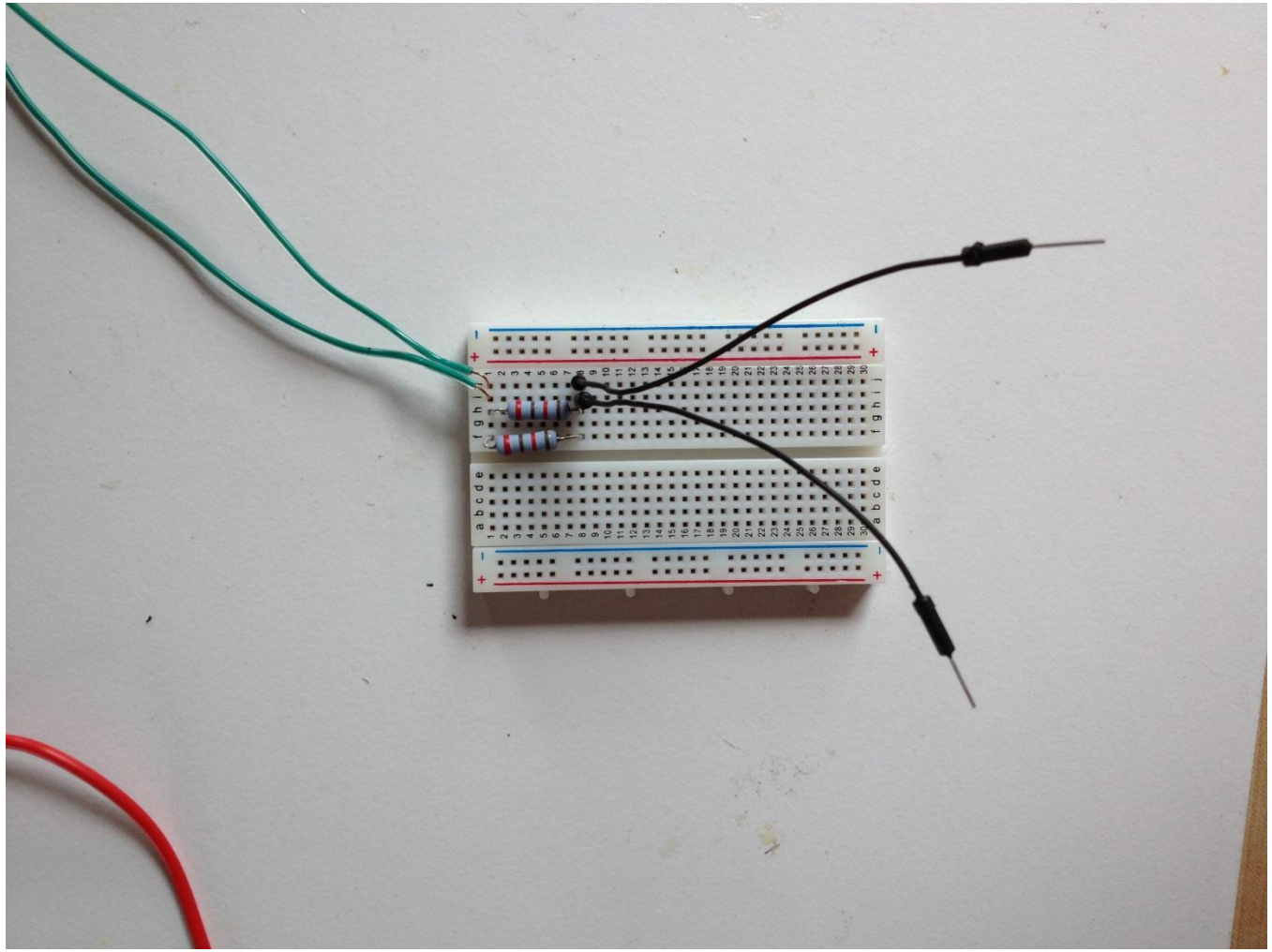
CAN Basics

- CAN-H (dominant) and CAN-L (recessive)
- Twisted pair wire
  - Does not _HAVE_ to be over short distances
- Terminated by two 120ohm resistors

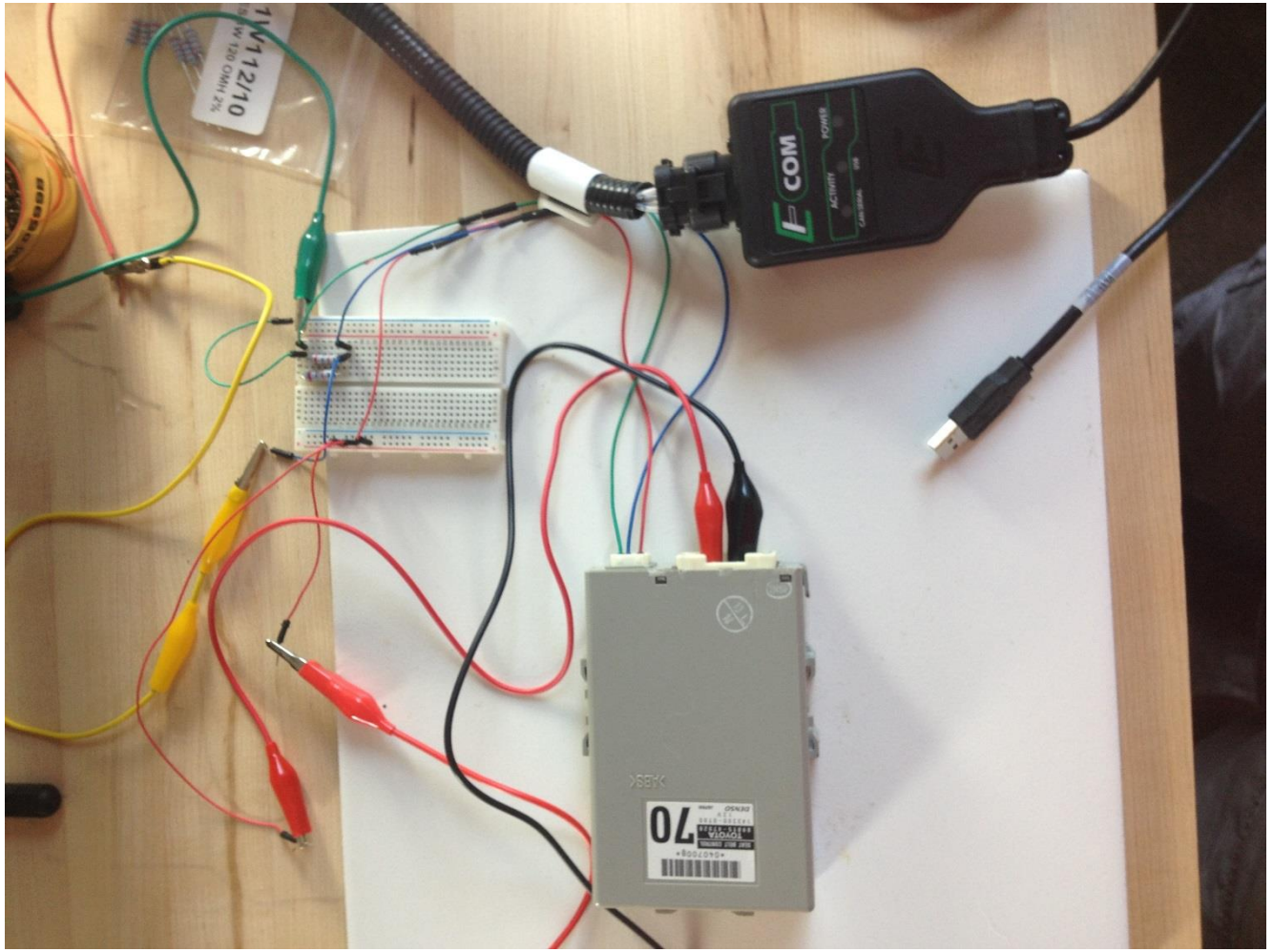


http://www.ni.com/cms/images/devzone/tut/a/5ca99f541439.gif

CAN Basics: Breadboard



CAN Basics: ECOM Cable



ECUBasics

Physical Edition

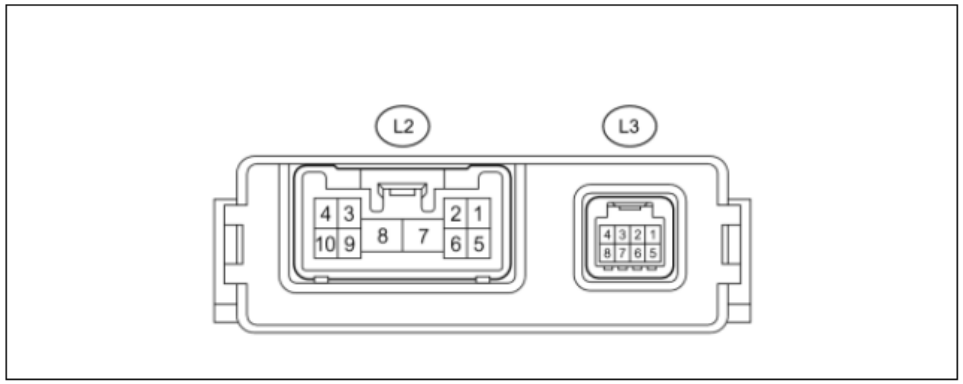
ECU Basics

- Minimally need power, ground, CAN-H, CAN-L to see traffic
  - Sometimes multiple power (+) lines will be required
  - Cars have battery and ignition, which you can run positive to both
- CAN-H & CAN-L
  - Some ECUs may have multiple pairs, for example Gateway ECUs
  - Others use multiple pairs for sub-networks (example: Toyota LKA)
- Wiring diagrams and mechanics accounts
  - http://www.i-car.com/html_pages/technical_information/technical_info.shtml
- Hooking these up appropriately should be enough for the ECU to emit its traffic
  - Potentially response to diagnostic messages
- Honestly, this usually isn't enough to get real-world results

ECU Basics: Harness Diagrams

TERMINALS OF ECU

1. CHECK SEAT BELT CONTROL ECU



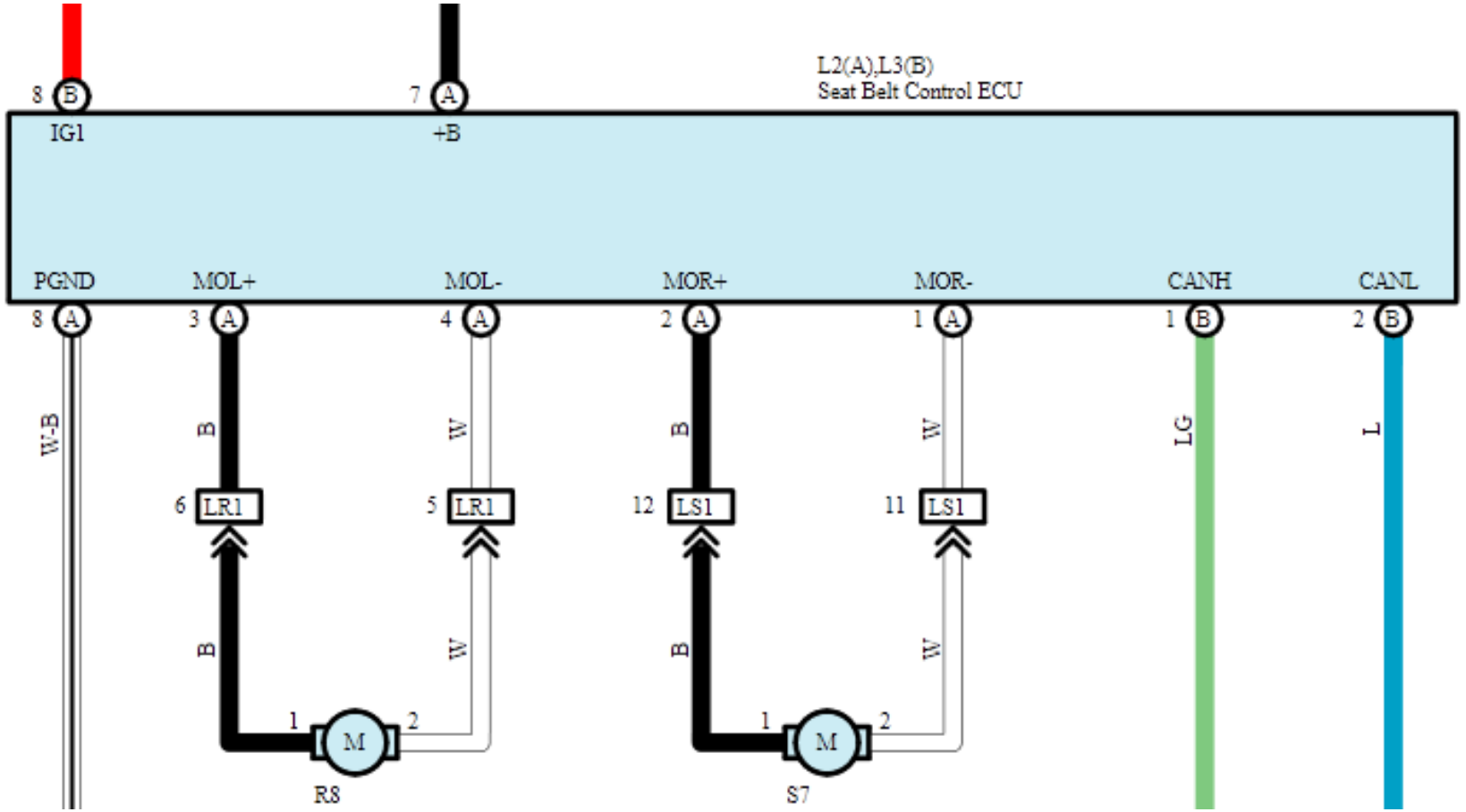
(a) Disconnect the seat belt control ECU connectors.

(b) Measure the resistance and voltage according to the value(s) in the table below.

TERMINAL NO. (SYMBOL)	WIRING COLOR	TERMINAL DESCRIPTION	CONDITION	SPECIFIED CONDITION
L2-7 (+B) - Body ground	B - Body ground	Battery voltage	Always	11 to 14 V
L2-8 (GND) - Body ground	W-B - Body ground	Body ground	Always	Below 1 Ω
L3-8 (IG1) - Body ground	R - Body ground	Seat belt control ECU power supply	Power switch on (IG)	11 to 14 V
			Power switch off	Below 1 V

https://techinfo.toyota.com/t3Portal/resources/jsp/siviewer/index.jsp?dir=rm/RM1290U&href=xhtml/RM000000VVK01BX.html&locale=en&model=Prius&MY=2010&keyWord=seat belt ecu&t3id=RM000000VVK01BX&User=false&publicationNumber=RM1290U&objType=rm&docid=1361488&context=ti

ECU Basics: Wiring Diagrams



https://techinfo.toyota.com/t3Portal/ewdappu/index.jsp?ewdNo=EM1290U&model=Prius&MY=2010&keyWord=seat belt ecu&locale=en&systemcode=SYS037&t3id=EM1290U_SYS037&User=false&publicationNumber=EM1290U&objType=ewdappu&docTitle=Vehicle+Interior%3A+Pre-Collision+System%3B+2010+MY+Prius+%5B04%2F2009+-+%5D&docid=1080347&context=ti

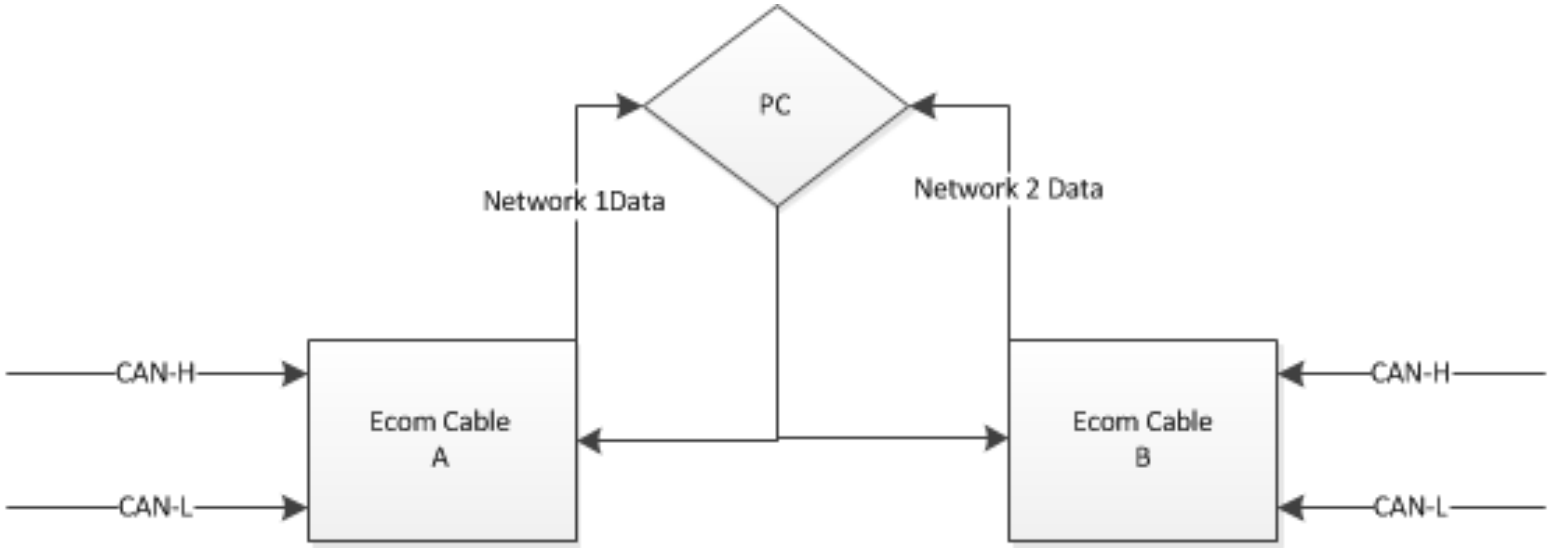
ECU Isolation

The Hard Way

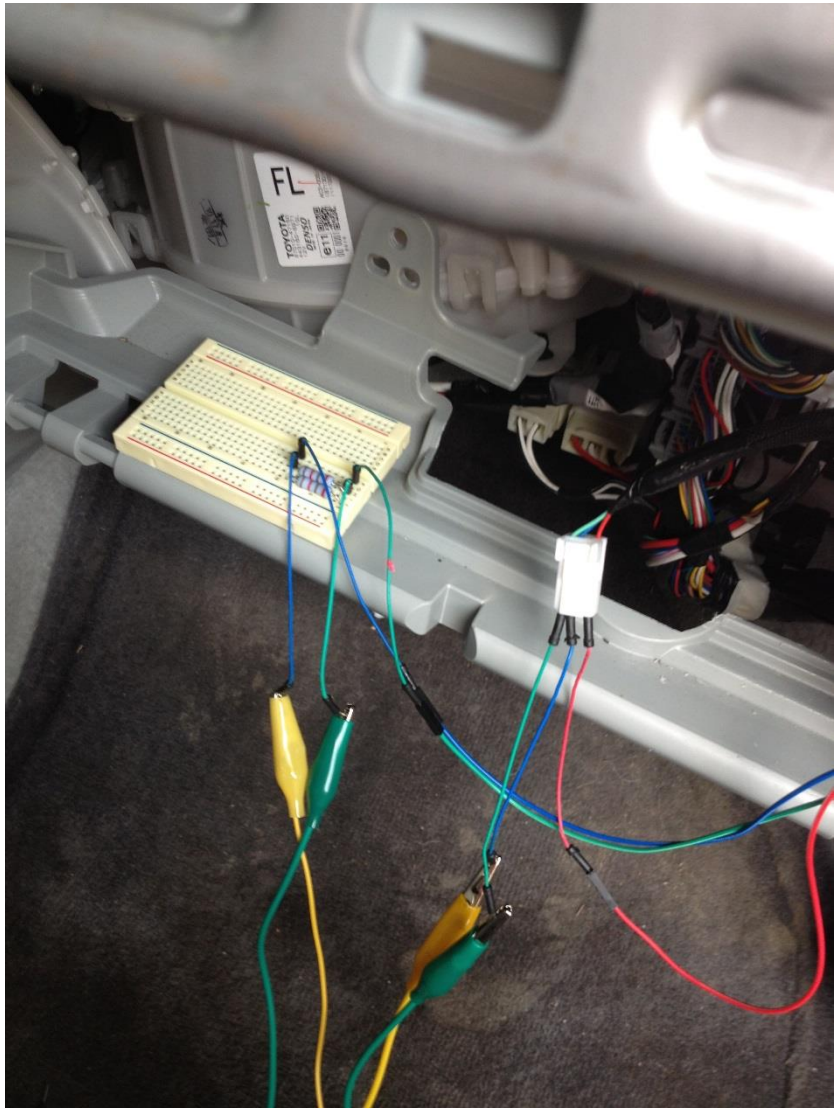
ECU Isolation: CAN Bridge

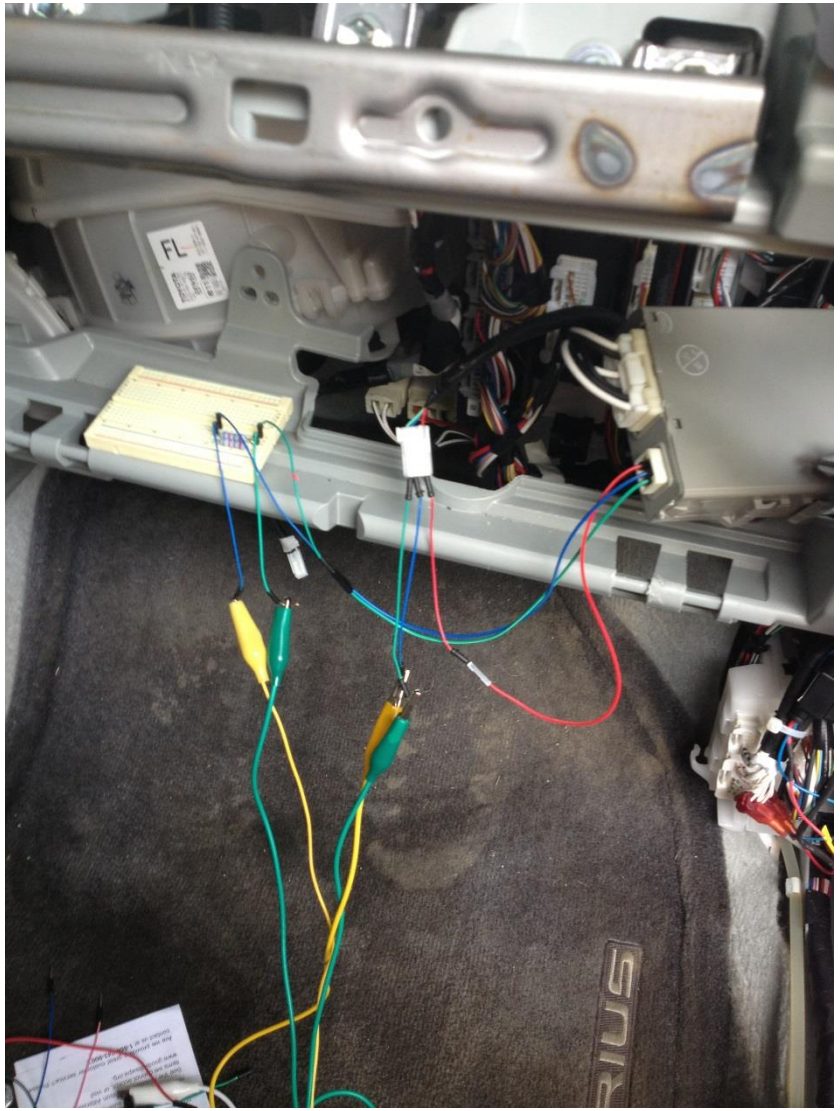
- We figured ECU in the car == fully functional
- We could then see which messages it was spitting out
- Pass them along to the bus
- Pass the traffic from the bus to the ECU

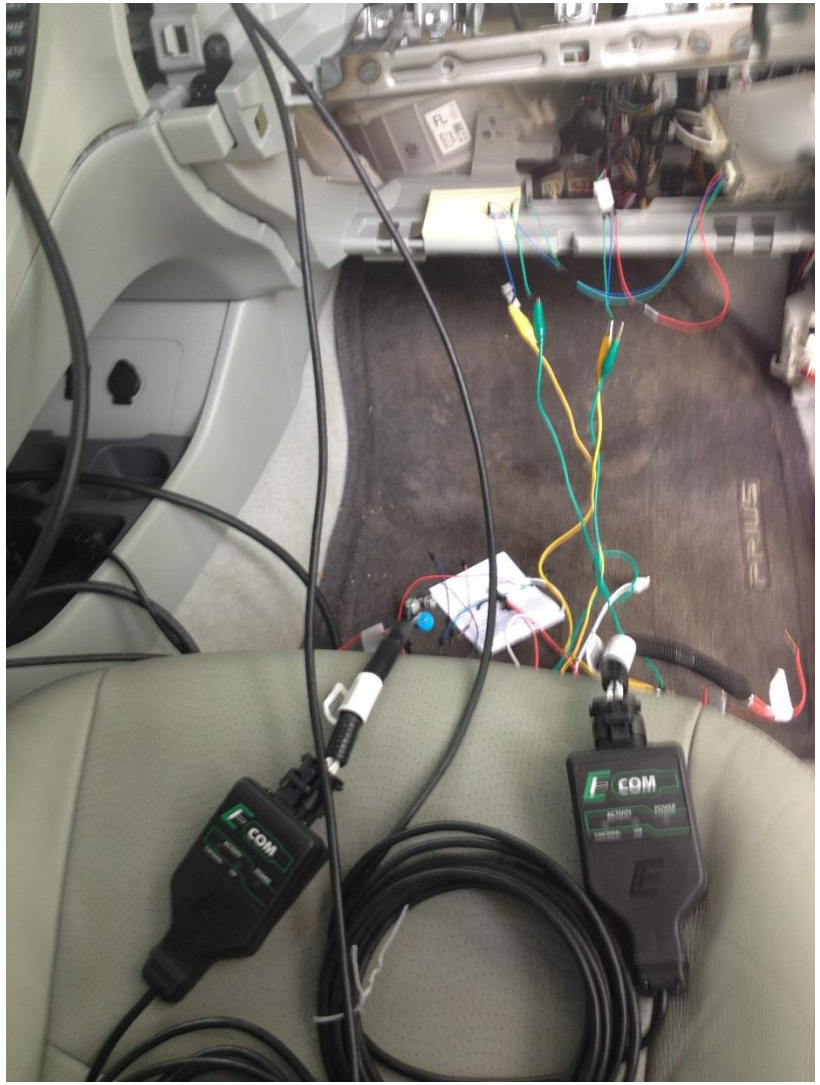
ECU Isolation: CAN Bridge



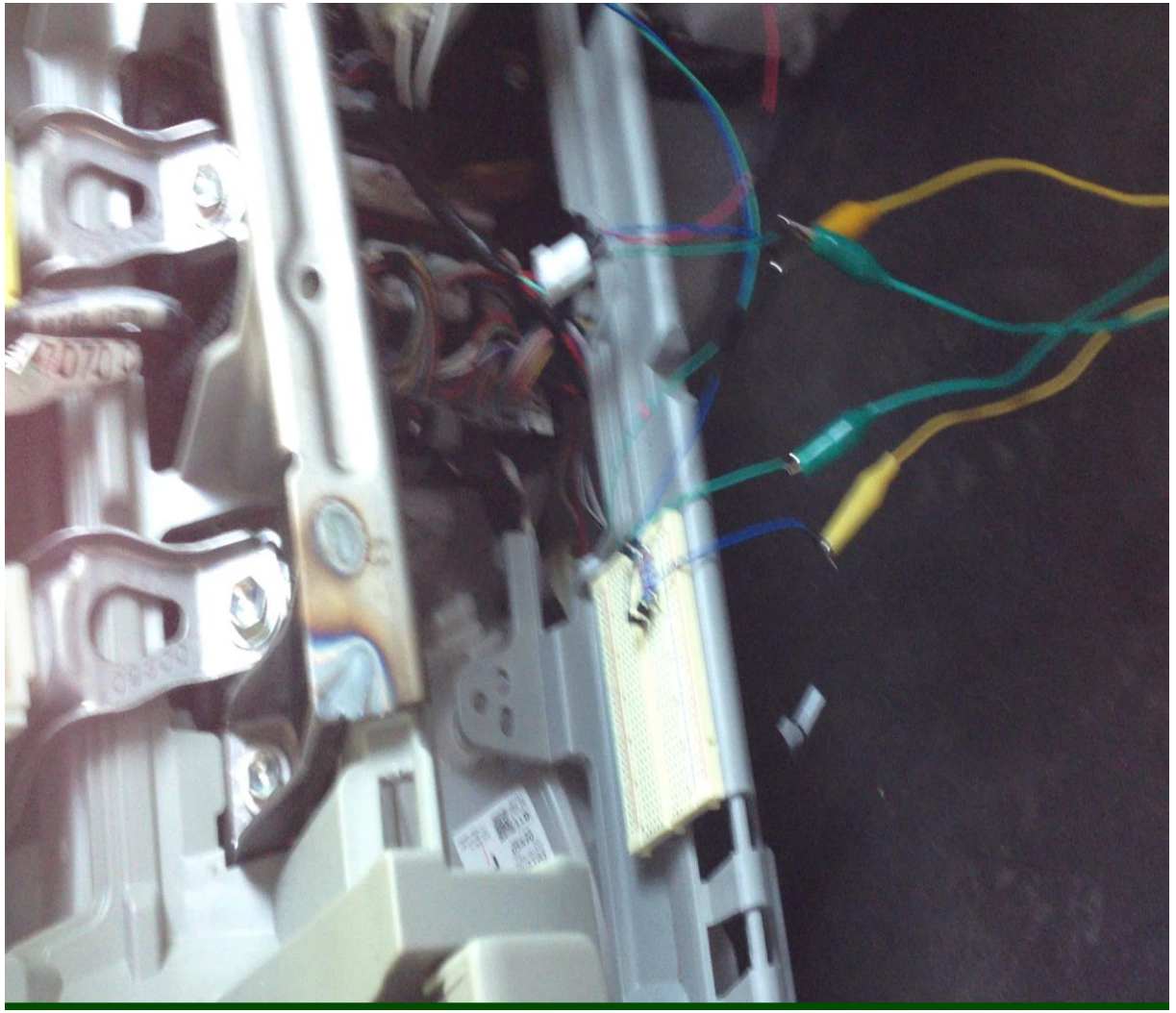
ECU Isolation: CAN Bridge II







ECU Isolation: CAN Bridge III



ECU Isolation: CAN Bridge

- Pros
  - Isolate ECUs in the car; know that all the other inputs/outputs are correct
  - Ability to modify or filter data
    - I think this is similar to what people are releasing at BH Asia
- Cons
  - Still requires a car
  - Ecom->PC->Ecom is very slow and CPU intensive
  - Not very practical if you're going to clip or modify wires
- What is the solution?

ECU Isolation

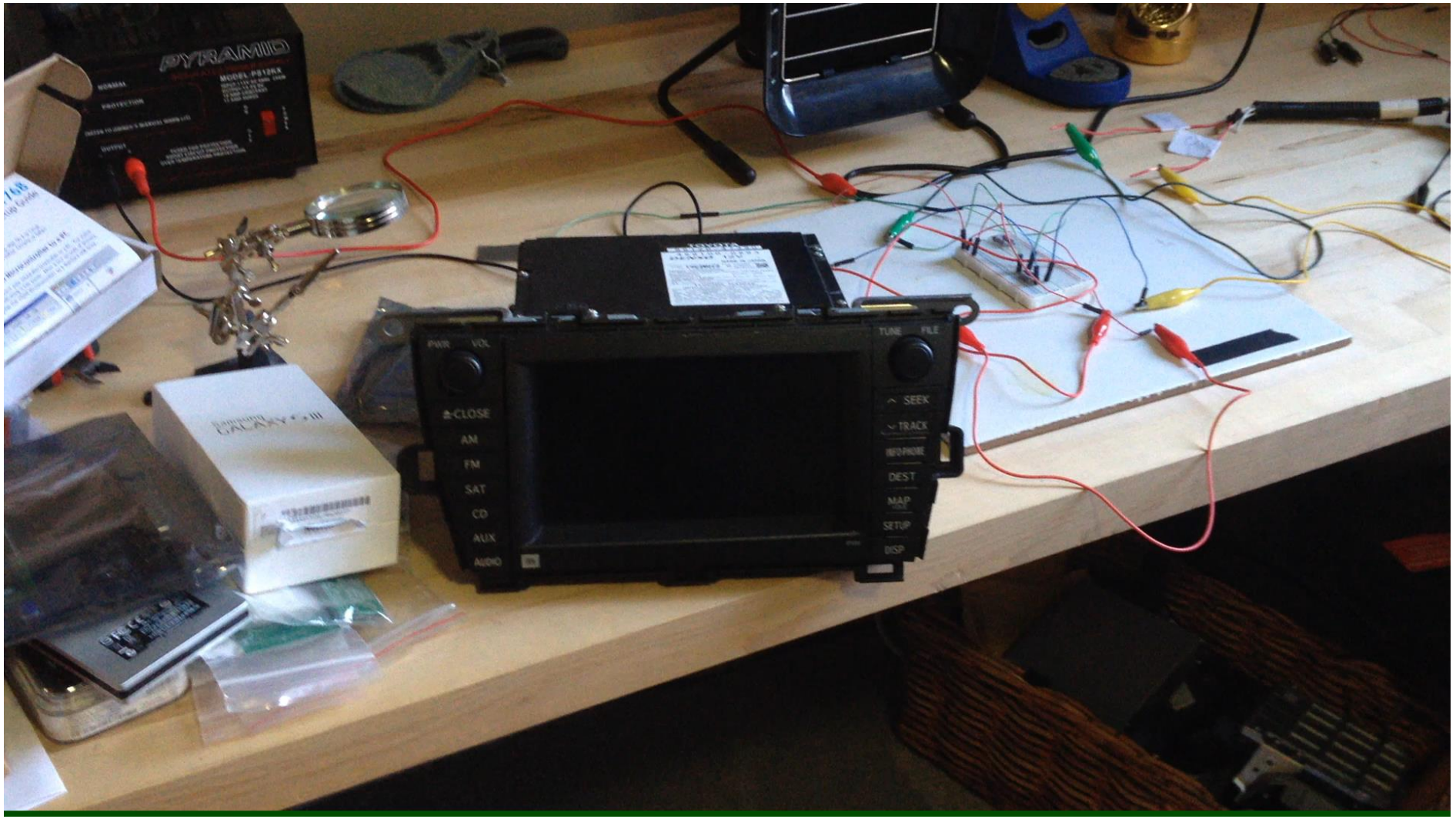
The Right Way

ECU Isolation: The Workbench

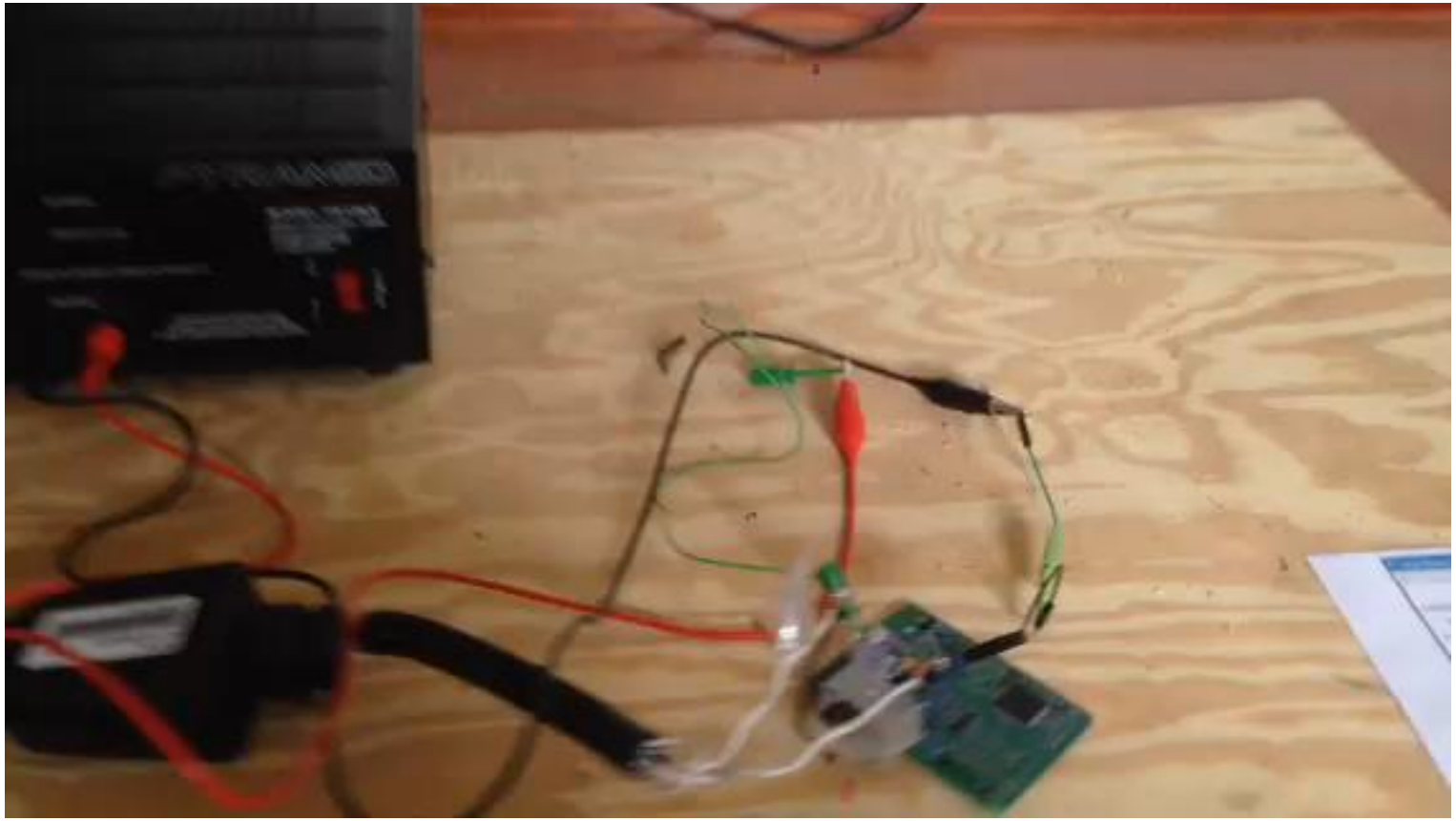
- Remove ECUs from the automobile all together
  - This also permits you to buy ECUs online w/o a car
- Use wiring diagrams and harness information to setup a single ECU
- We now have isolated ECUs that will emit traffic working outside of the vehicle
- Just because it ‘turns on’ doesn’t mean it’s working…

ECU Isolation: Real Life

ECU Isolation: Does it work? | AV



ECU Isolation: Does it work? | Emit Traffic



ECU Isolation: Is it REALLY working?

- Best way is to compare a capture made from a car with the ECU
  - Not always possible, but you can rent/borrow a car for a capture
- Below is the seat belt ECU from the Prius

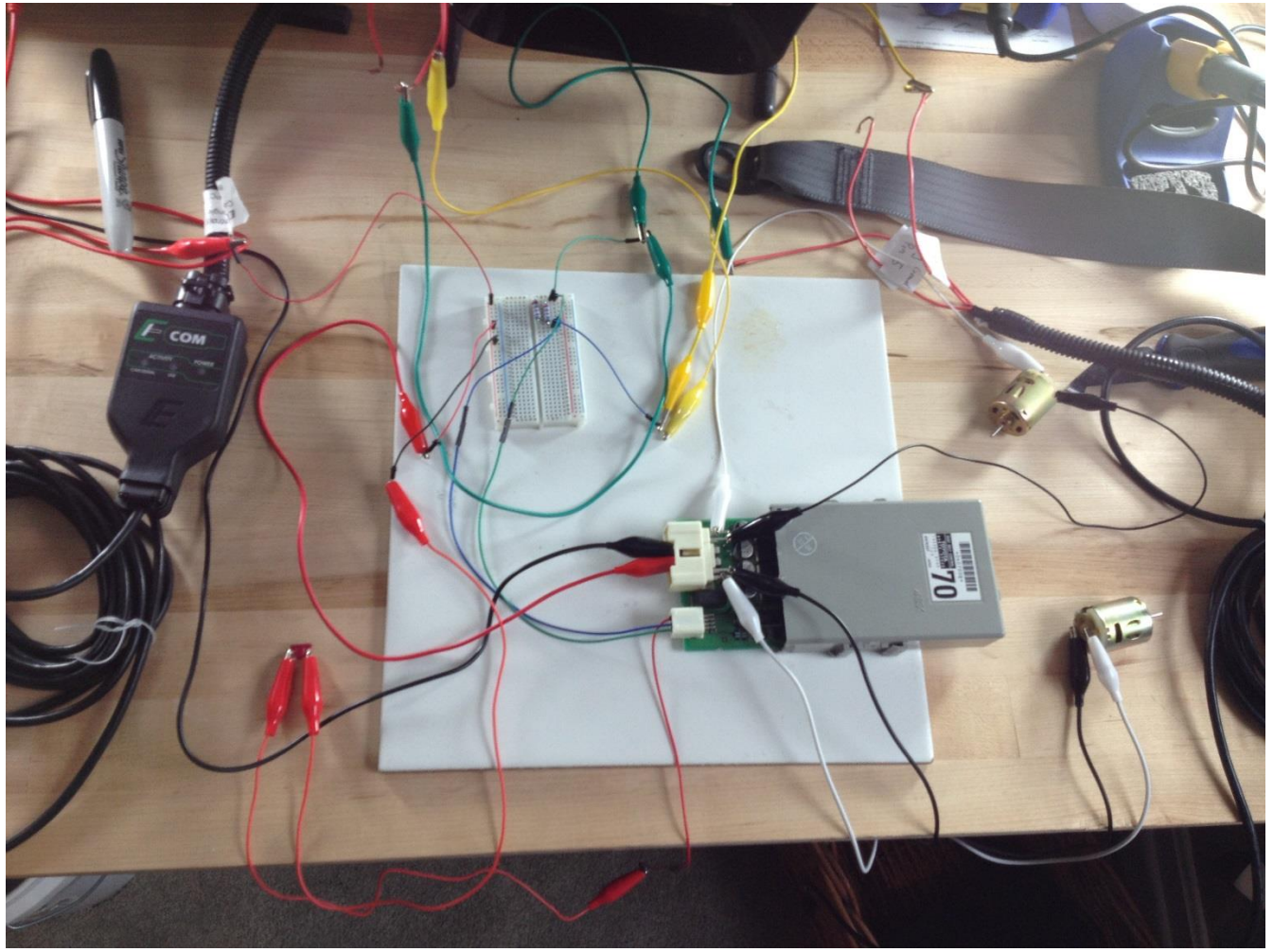
In Car (ODB-II)	On Bench (No sensors/actuators)
IDH: 03, IDL: 9C, Len: 01, Data: **08** TS: 35060	IDH: 03, IDL: 9C, Len: 01, Data: **08** ,TS: 28460,BAUD: 1
IDH: 03, IDL: 9C, Len: 01, Data: **08** TS: 50684	IDH: 03, IDL: 9C, Len: 01, Data: **08** ,TS: 44086,BAUD: 1
IDH: 03, IDL: 9C, Len: 01, Data: **08** TS: 66307	IDH: 03, IDL: 9C, Len: 01, Data: **09** ,TS: 59711,BAUD: 1
IDH: 03, IDL: 9C, Len: 01, Data: **00** TS: 81945	IDH: 03, IDL: 9C, Len: 01, Data: **01** ,TS: 75338,BAUD: 1
IDH: 03, IDL: 9C, Len: 01, Data: **00** TS: 97569	IDH: 03, IDL: 9C, Len: 01, Data: **01** ,TS: 90963,BAUD: 1
IDH: 03, IDL: 9C, Len: 01, Data: **00** TS: 113195	IDH: 03, IDL: 9C, Len: 01, Data: **01** ,TS: 106588,BAUD: 1
IDH: 03, IDL: 9C, Len: 01, Data: **00** TS: 128816	IDH: 03, IDL: 9C, Len: 01, Data: **01** ,TS: 122214,BAUD: 1

ECU Isolation

Making it Work

MiW: Attach Sensors / Actuators

- Why didn’t you poories already think of this?

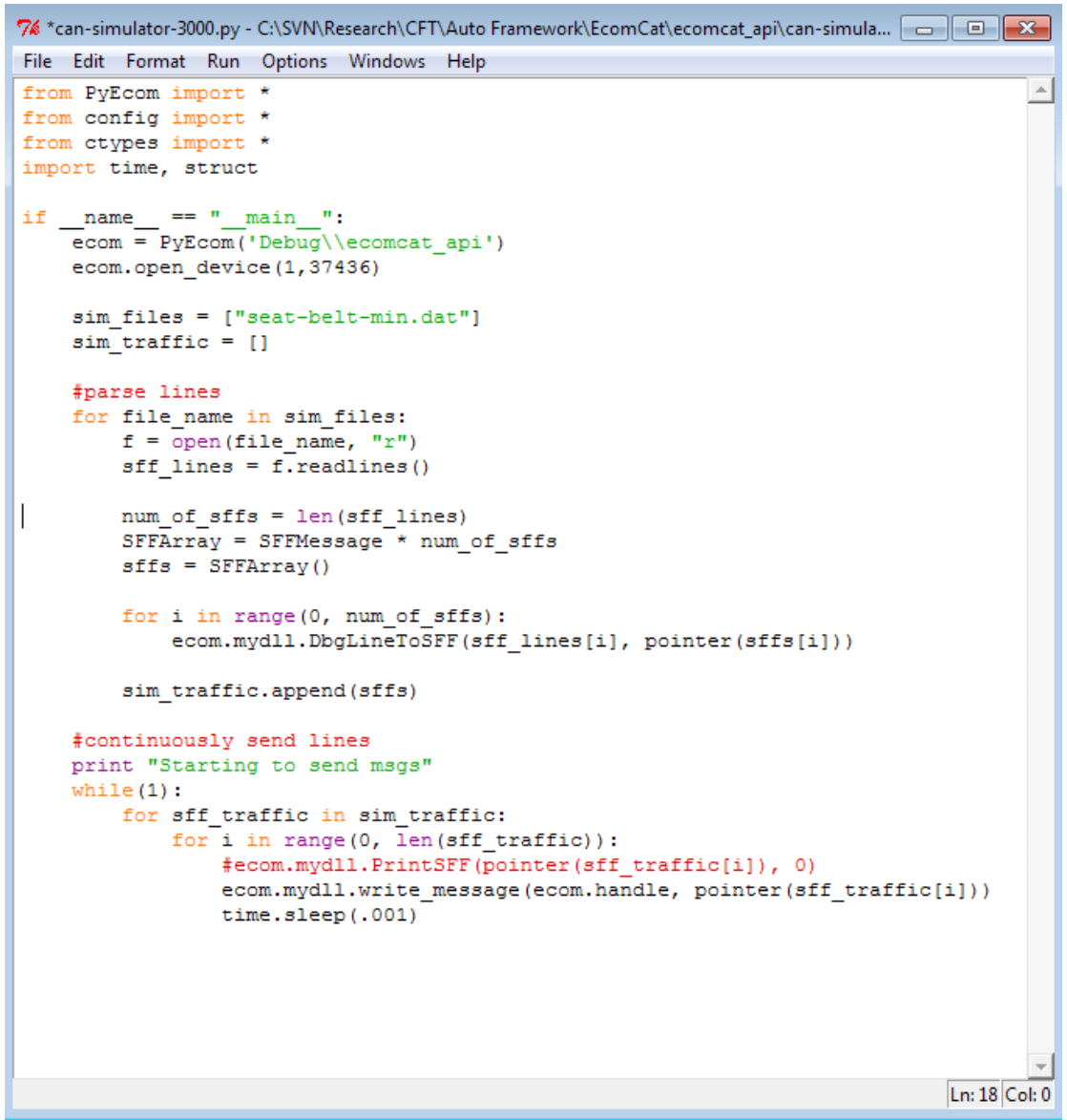


Too poor for sensors? Fake it

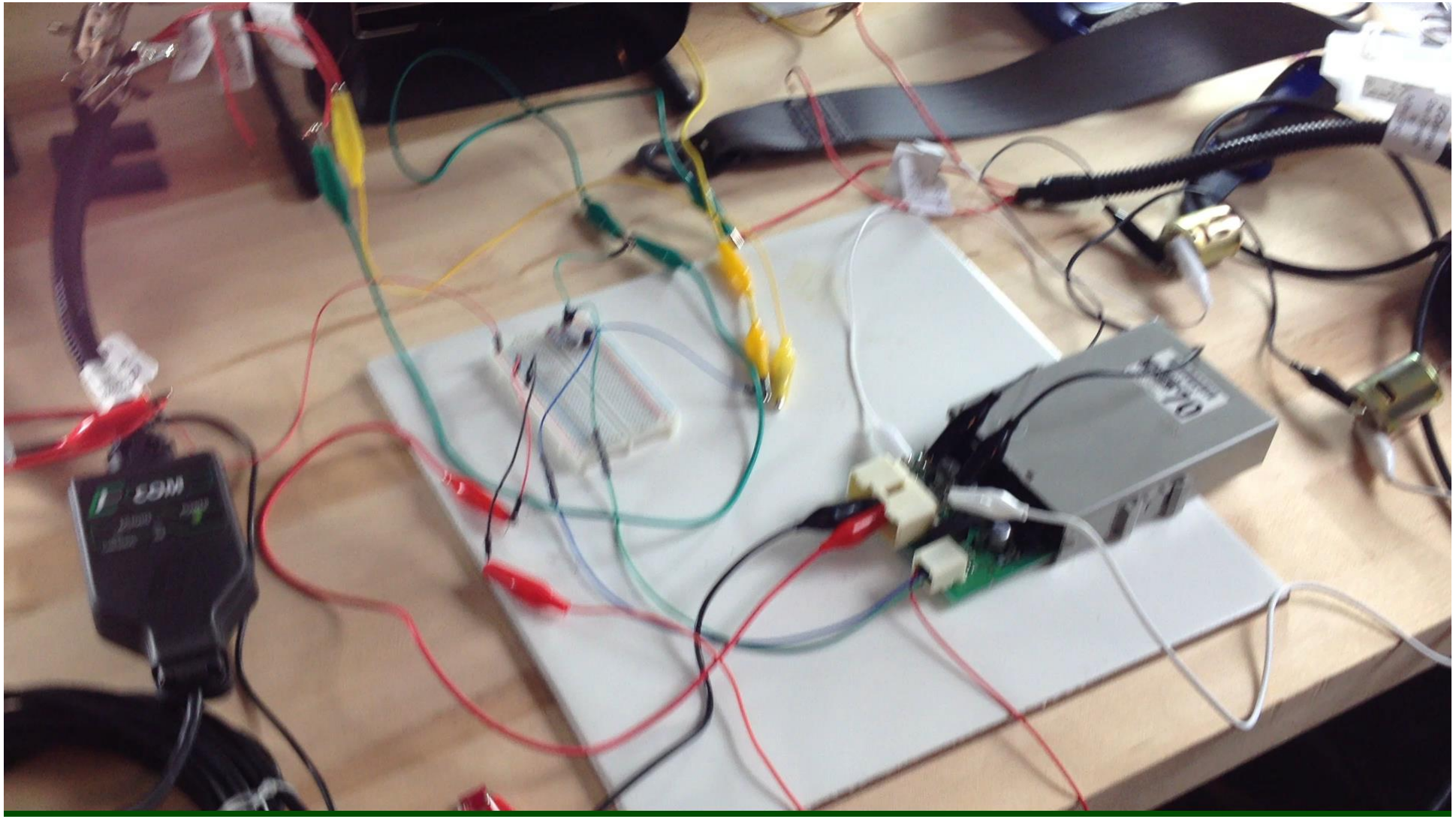
What else?

- ECUs need sensors and actuators to be happy
- In order to fully function, they also need CAN traffic
- In the year 3000……

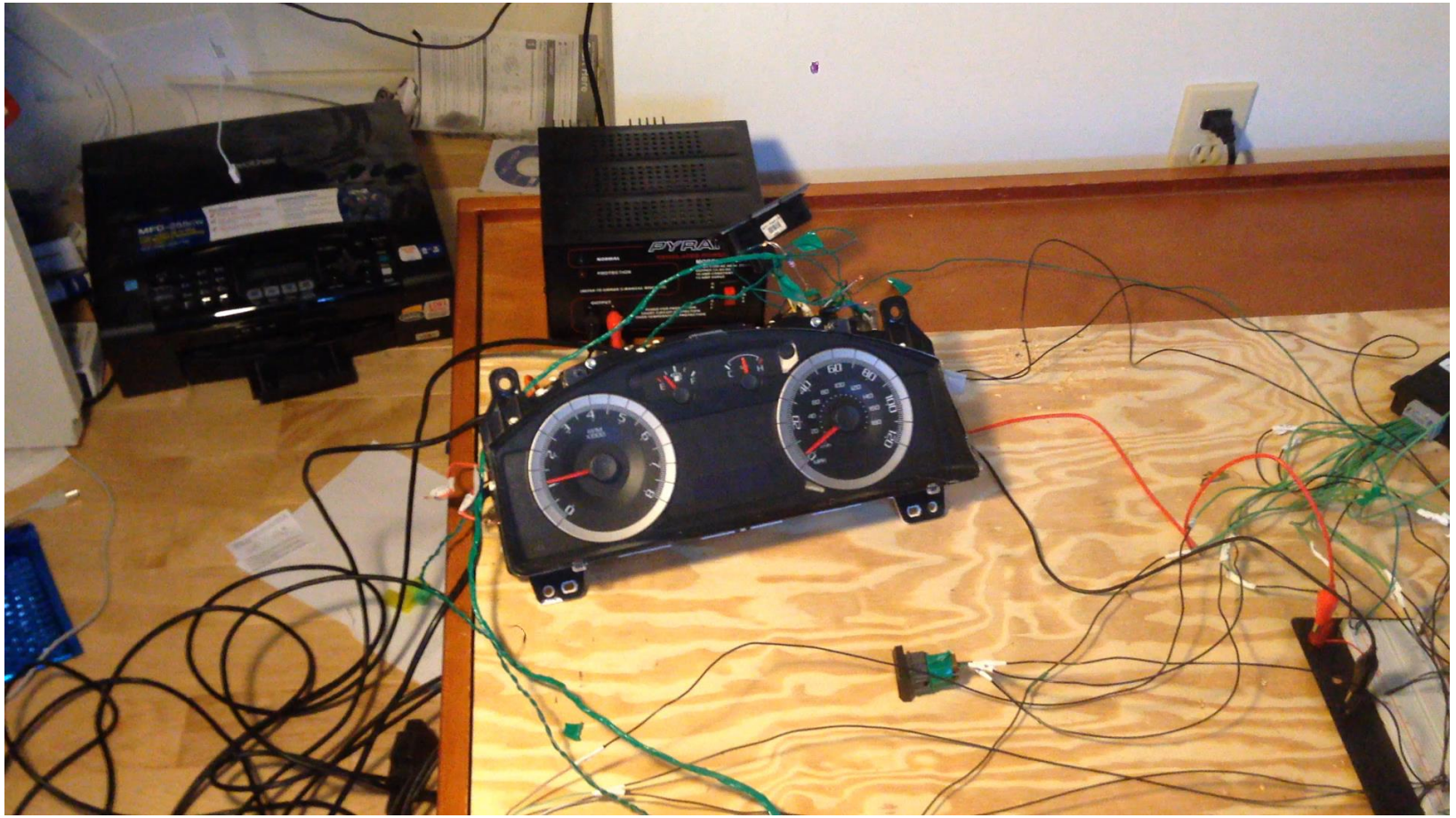
MiW: CAN-Simulator 3000



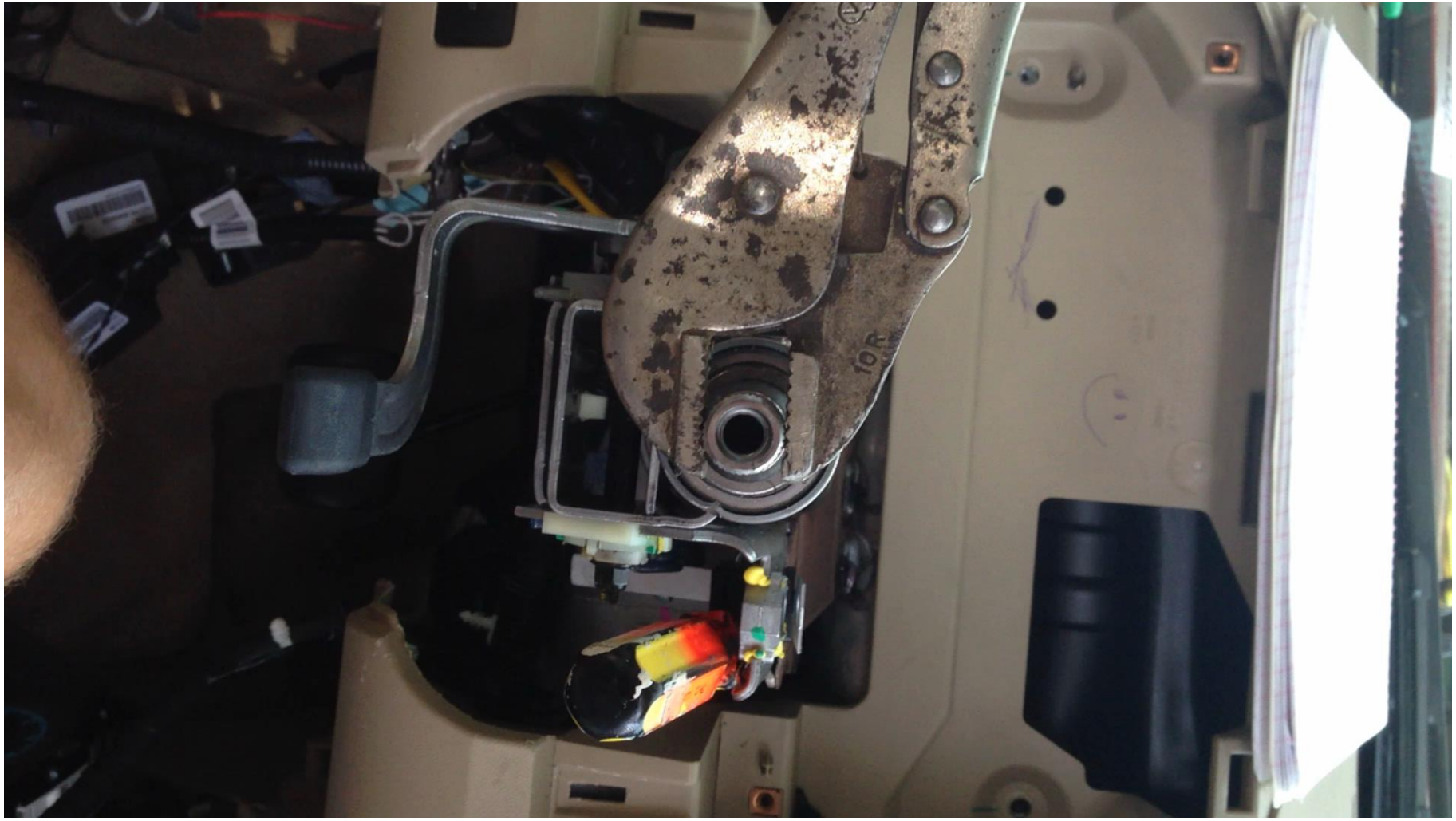
MiW: Real Life



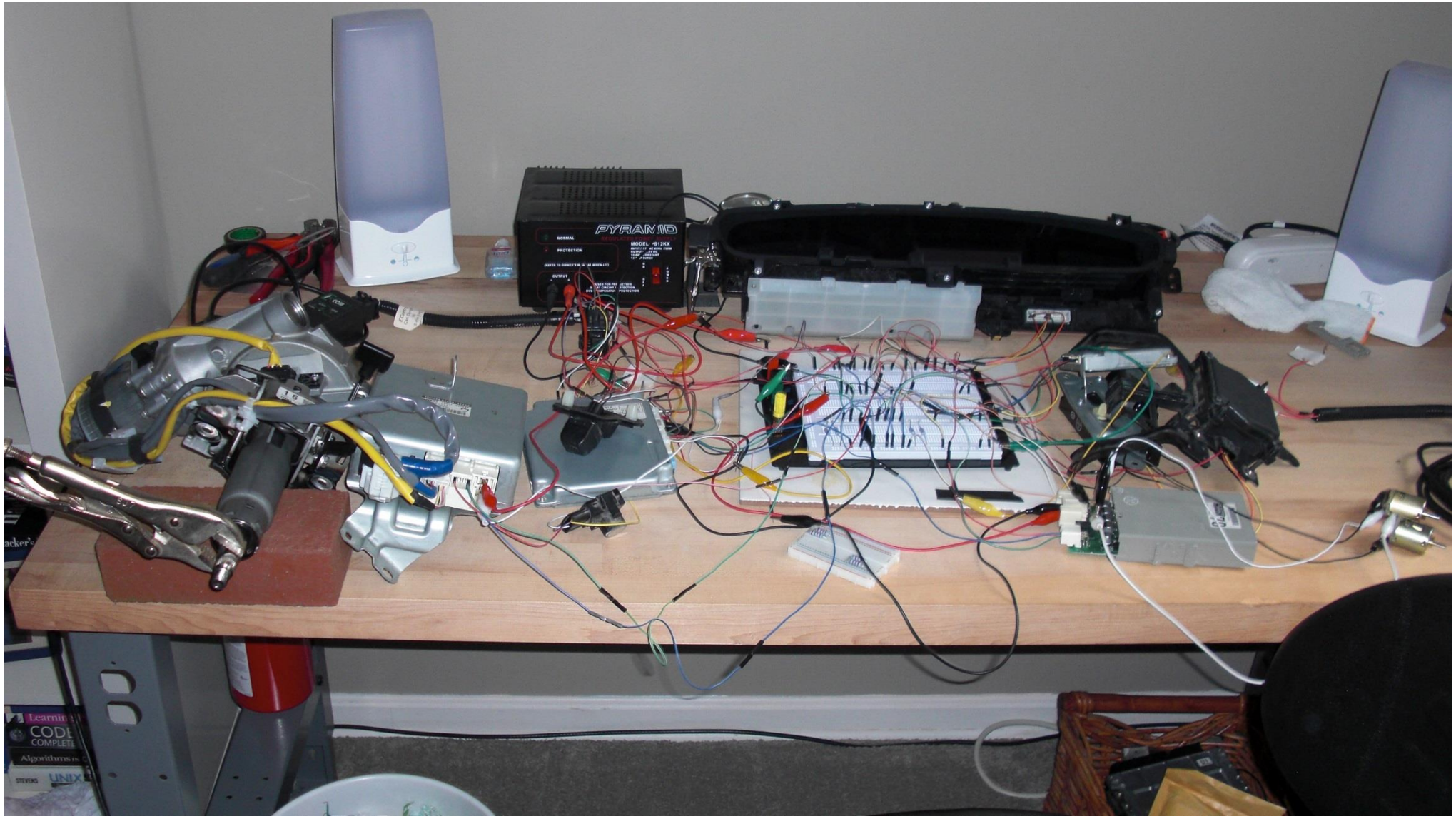
Sending messages for ECUs



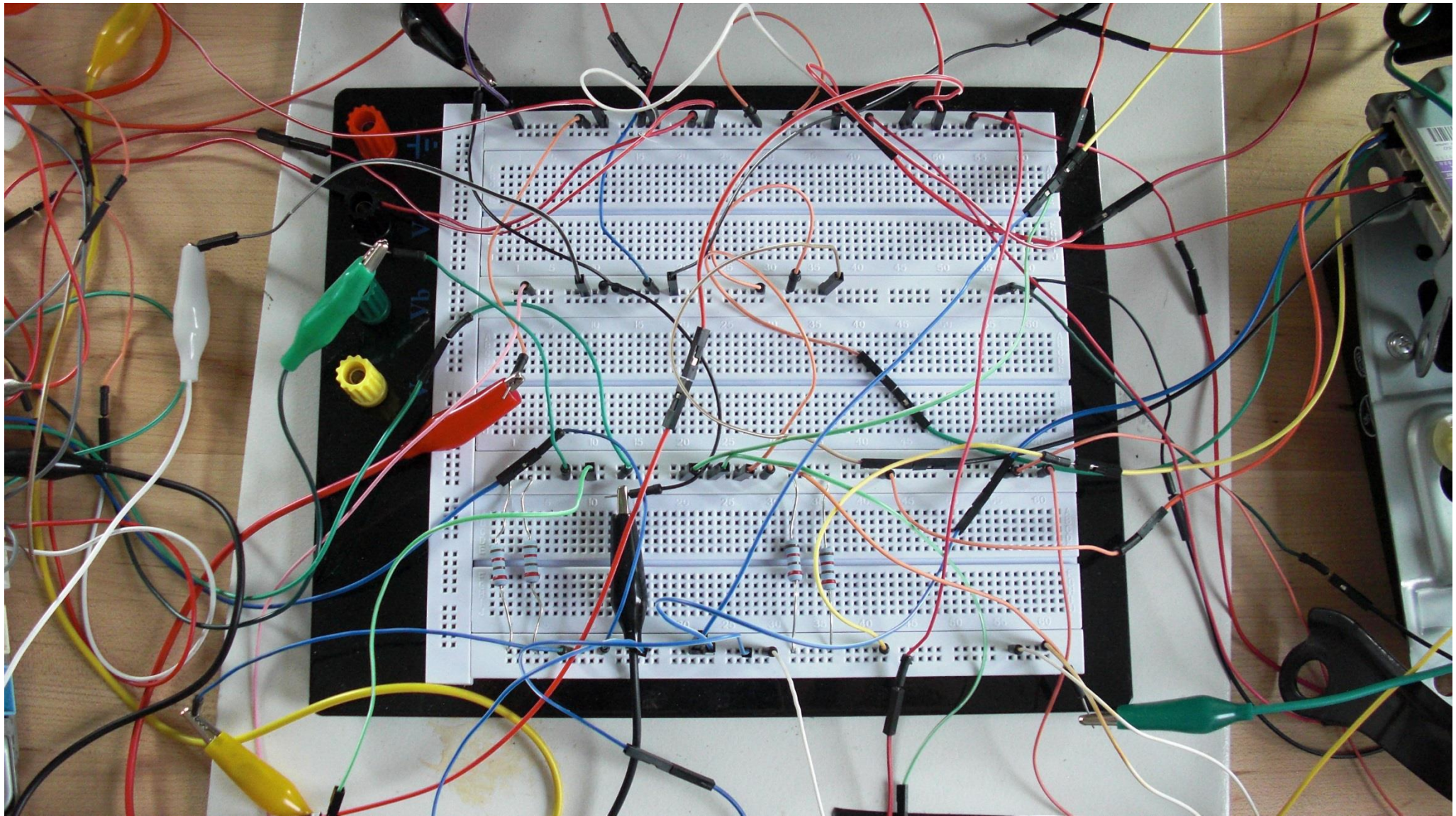
More messages!



MiW: Collect them All!



MiW: Collect them All!

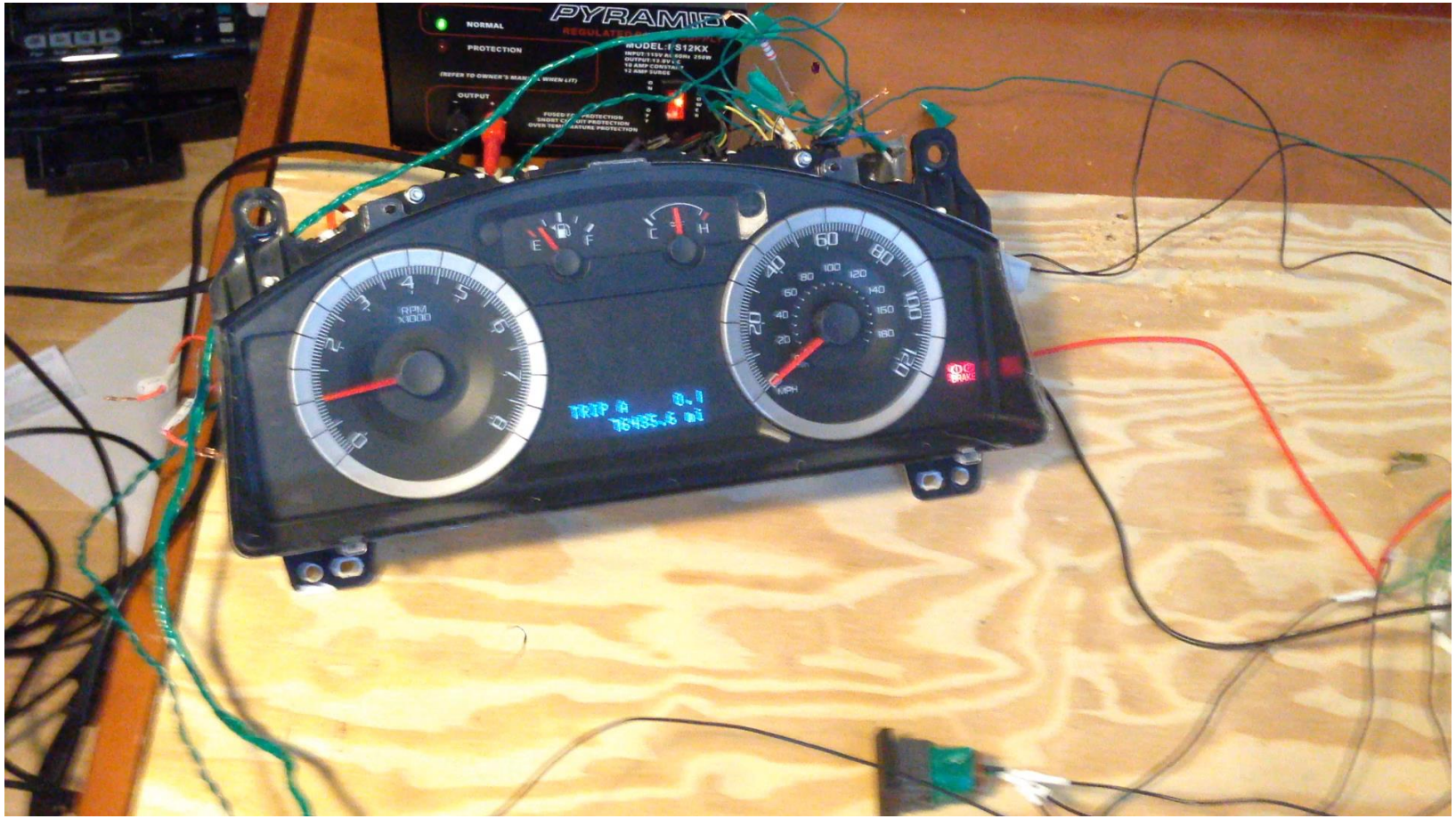


ECU Attacks

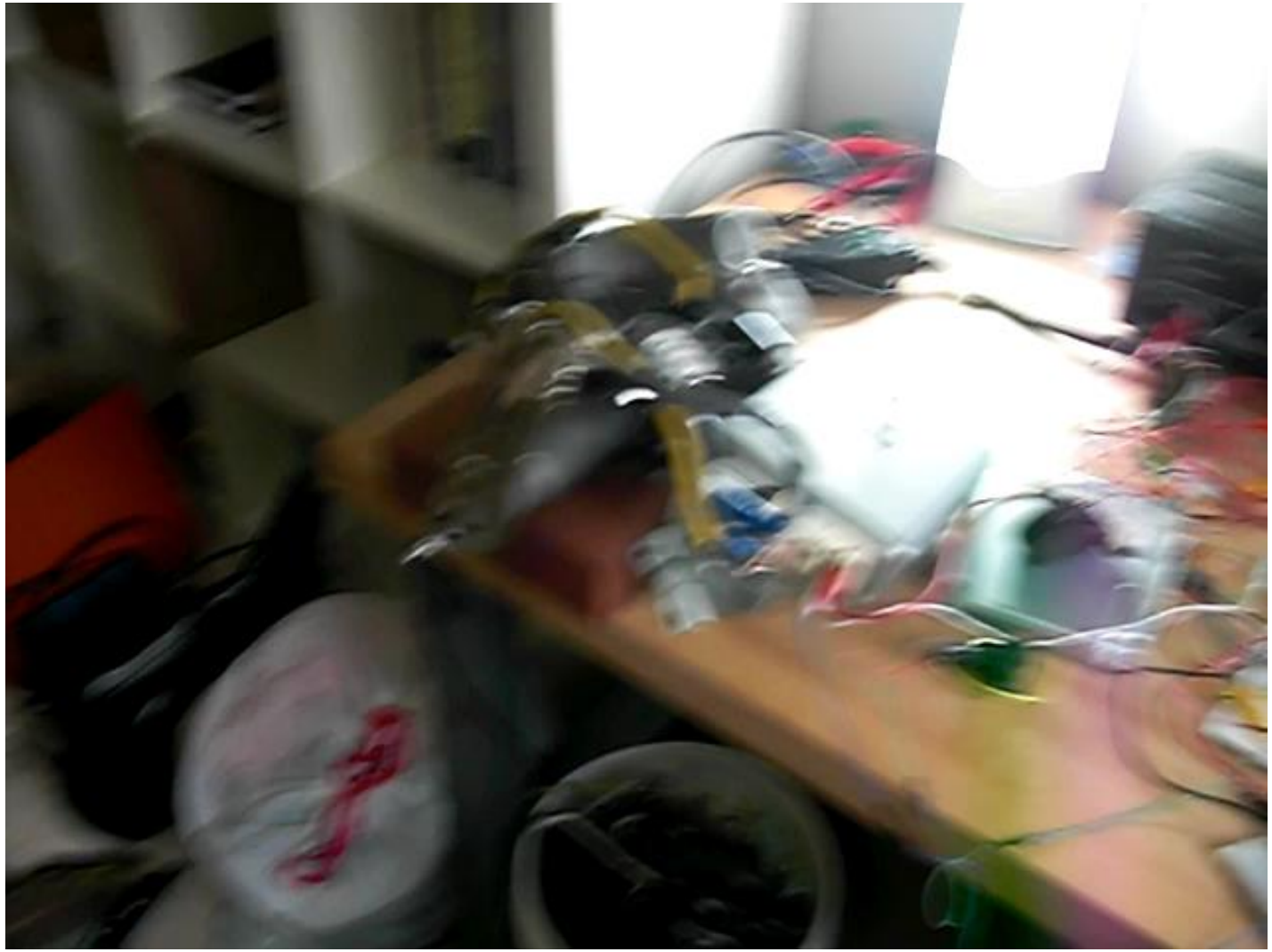
Hacking a car without a car

ECU Attacks: Instrument cluster

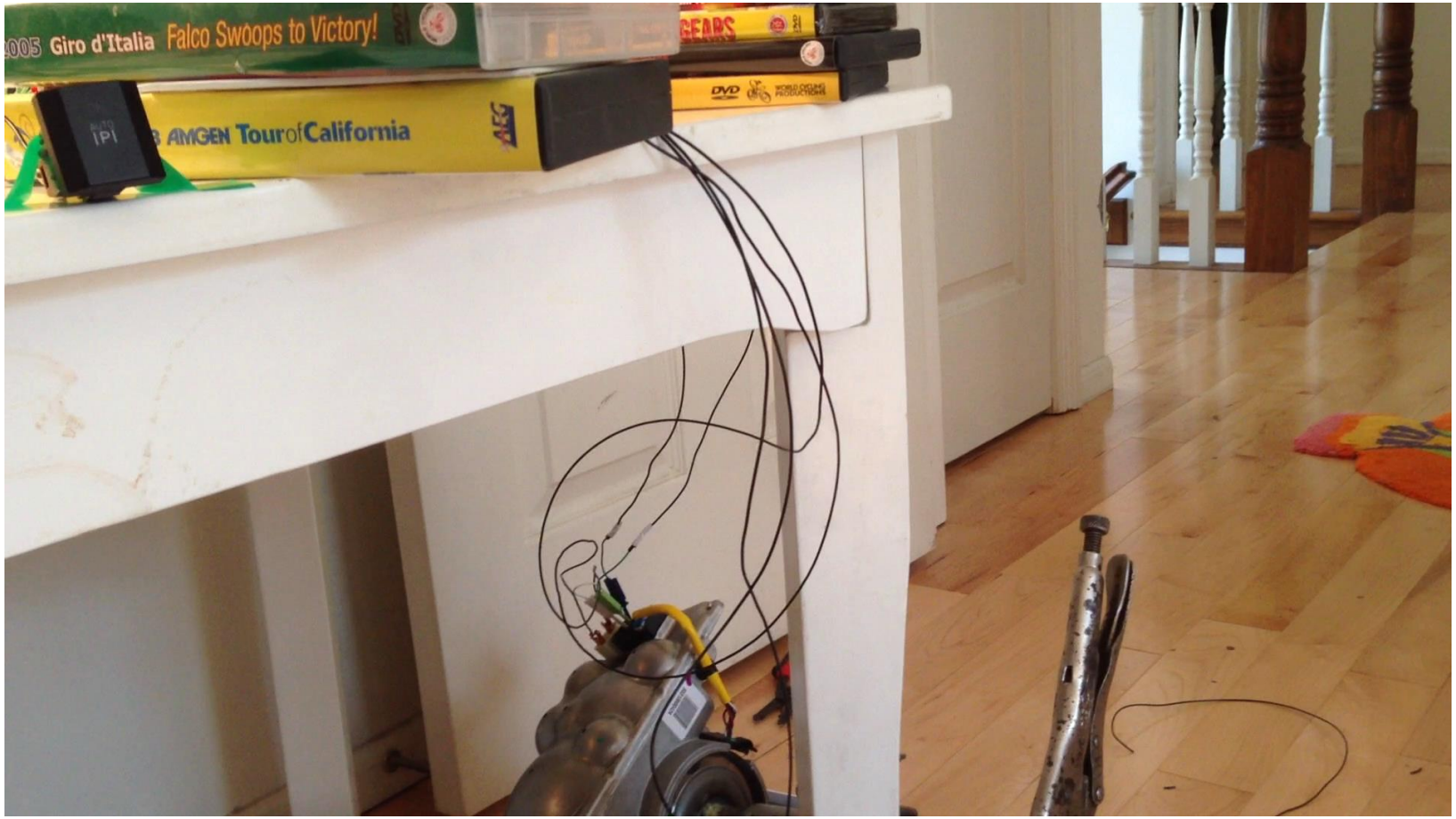
CAN injection - Ford speedometer



ECU Attacks: LKA

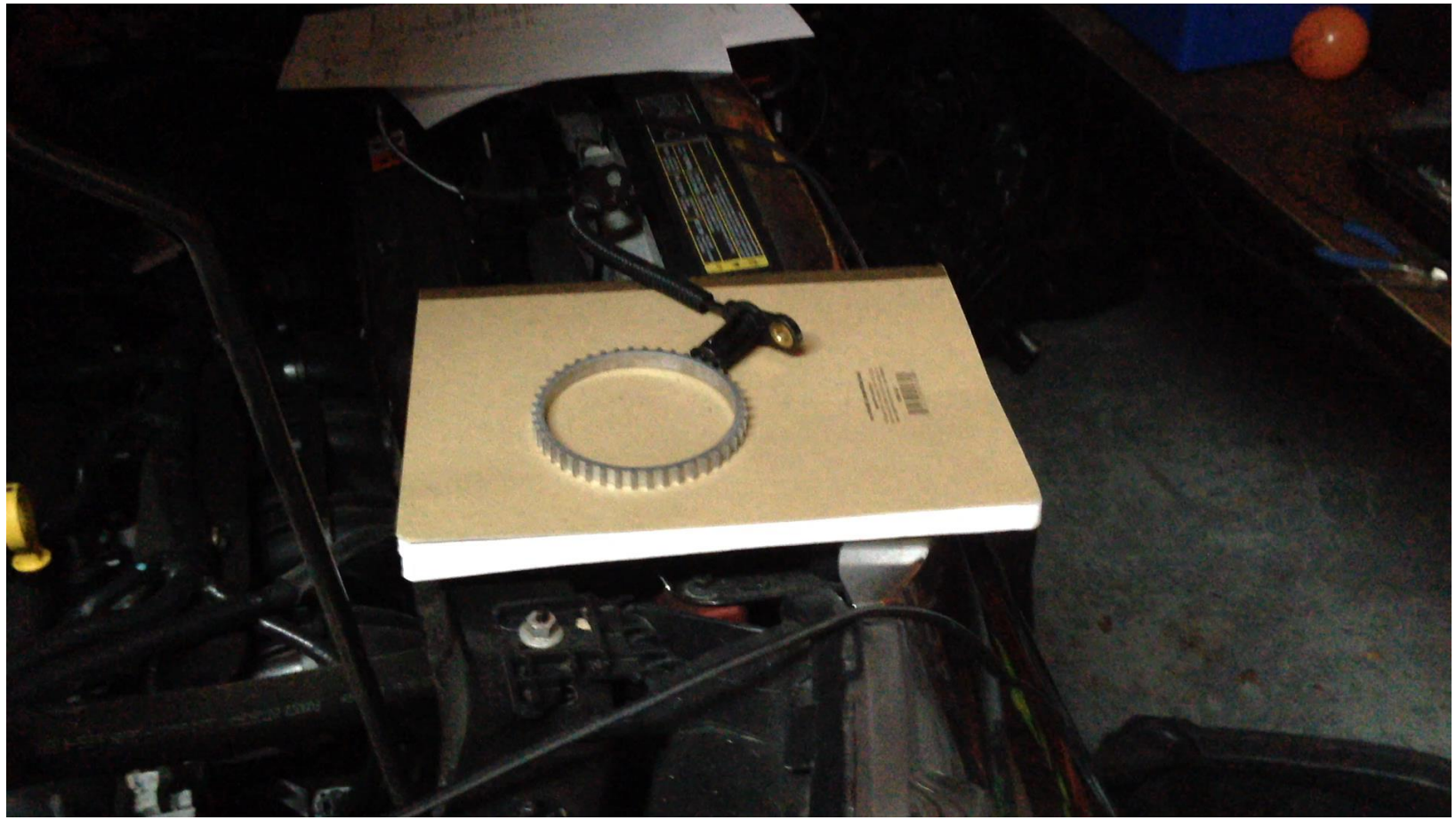


Ford steering on the bench

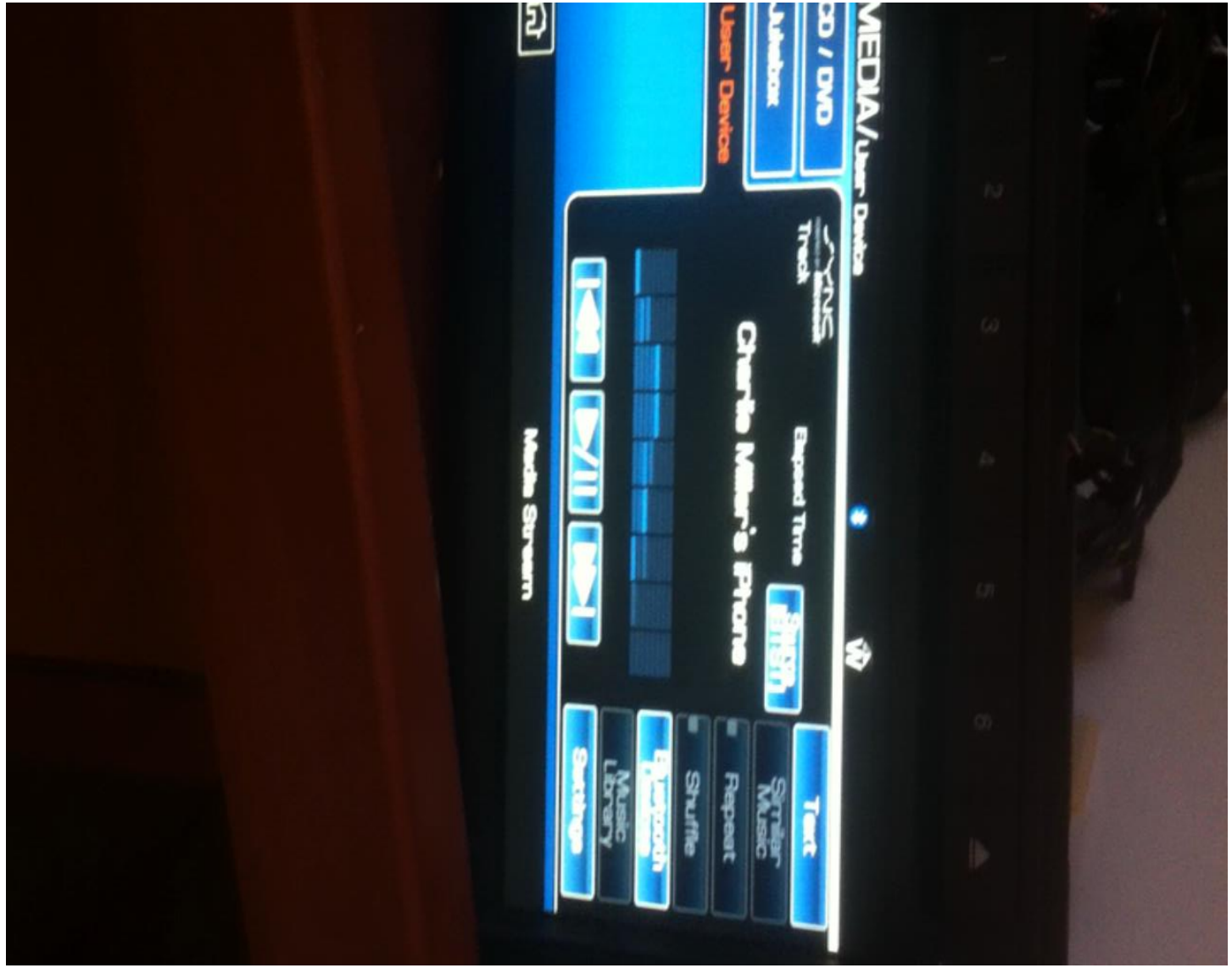


ECU Attacks: Back camera / sensors

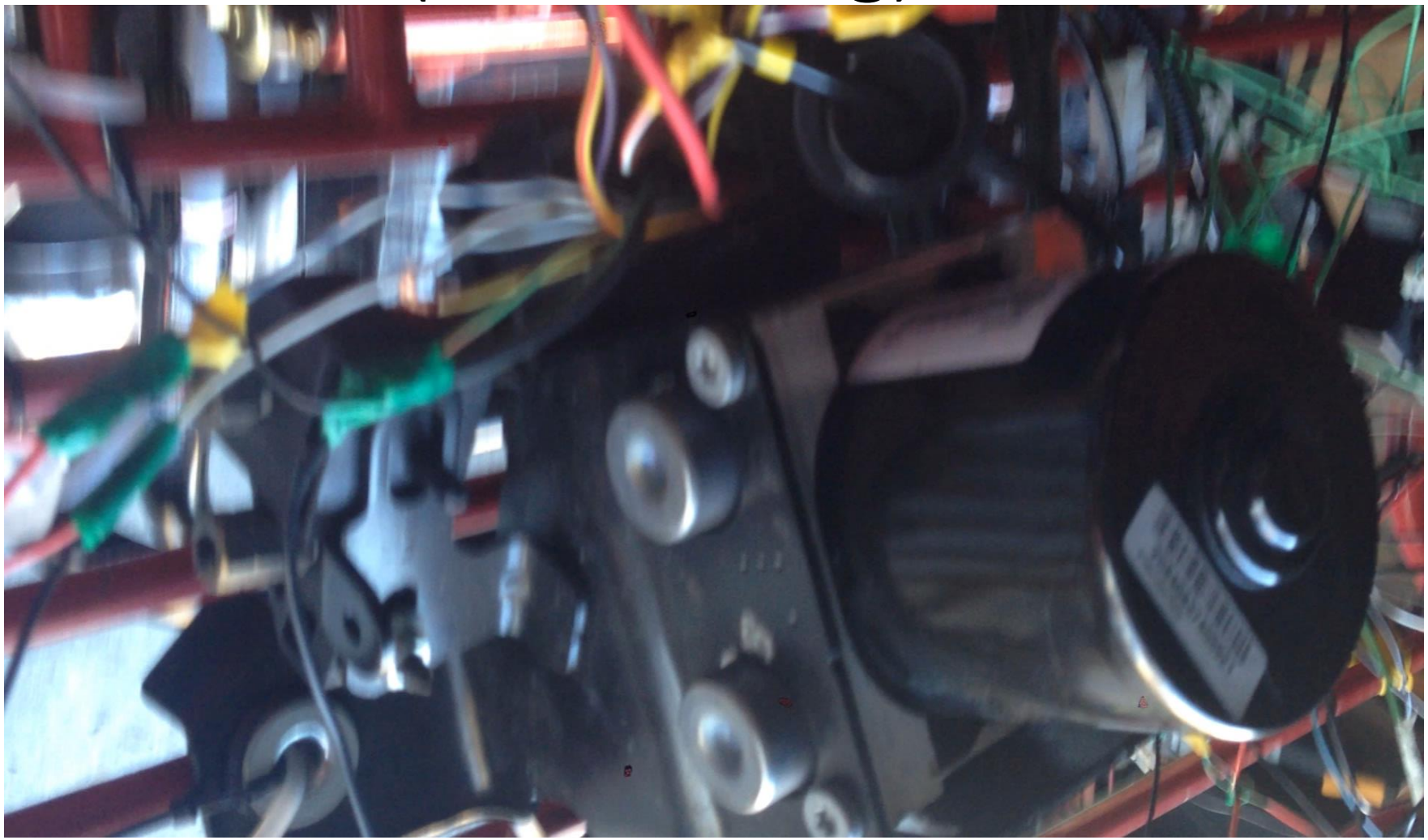
Wheel sensor in action



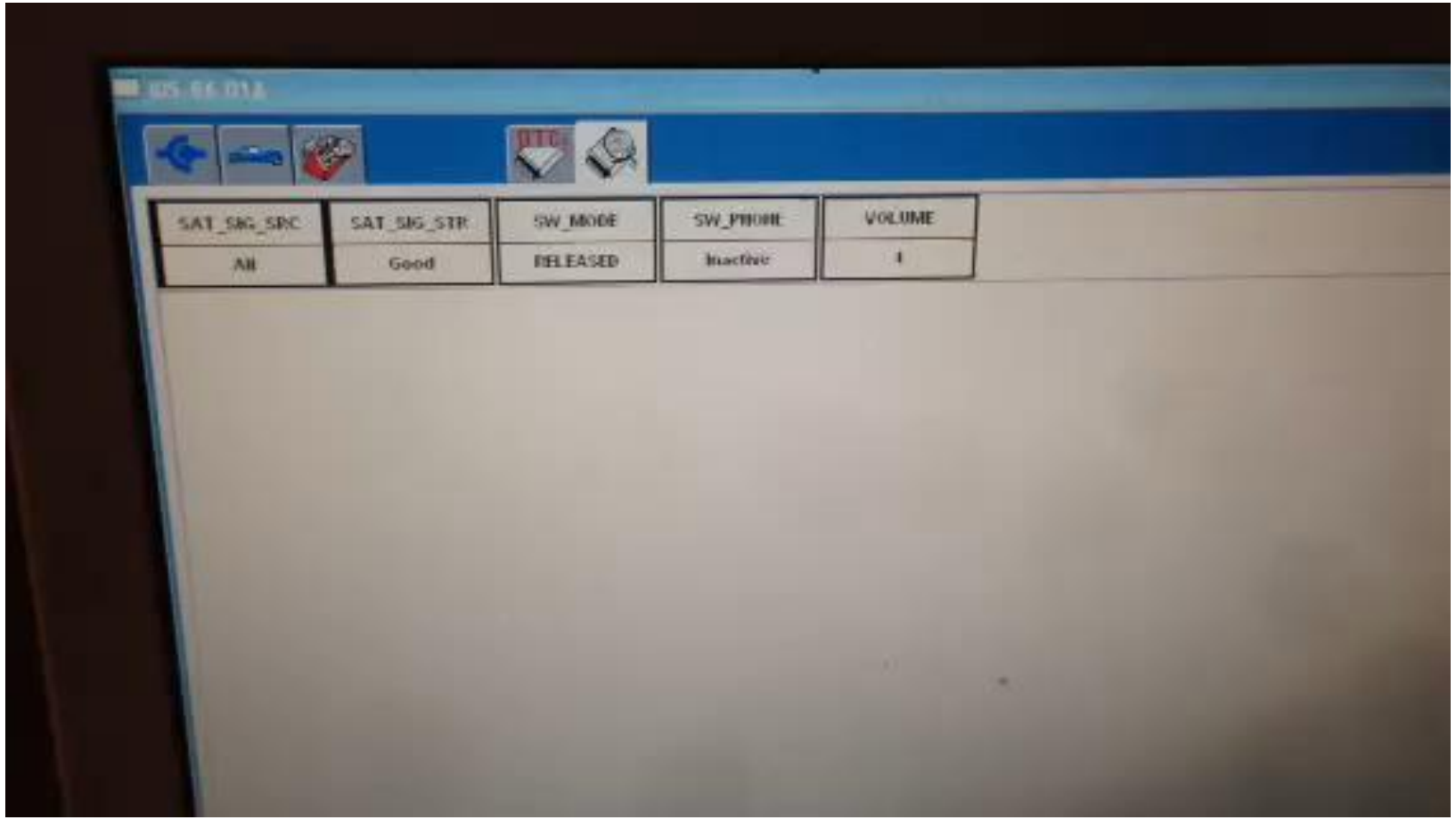
ECU Attacks: Infotainment



Disable brakes (via bleeding)



Mechanics tools over ODB-II



The Bench

The Bench: Pros

- CAN ID isolation saves you valuable time
  - Example: No more looking at a huge capture for steering packets
- Many diagnostic tests can be administered
  - Think securityAccess + mechanics tools
- Try attacks / fuzzing on the bench w/o fear for your life
- Remote attack research
  - Bluetooth, WiFi, Telephony, etc
- All without a car!*
  - *Might require a rental/zipcar to get baseline capture (no biggie)

The Bench: Cons

- Potentially need a baseline
- Hard to retrieve some items from the automobile
  - Engine, brakes, suspension, etc
- The bench does not move
  - Things like PCS require movement

Mobile Testing Platform

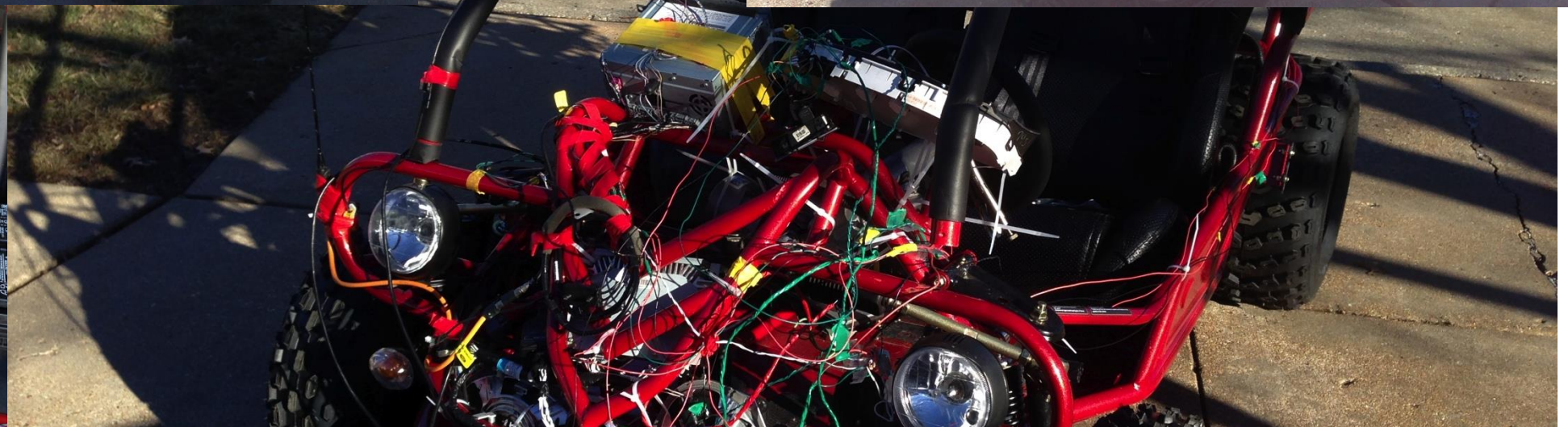
The Cart

The Cart: Base model

http://gokartsusa.com/kandi-150-kd-150fs-buggy-gokart.aspx

The Cart: Miller-Valasek Mods

Worlds most sophisticated gocart



The Cart: Miller-Valasek Mods

The Cart: Modifications

- Multiple CAN networks
- Sensors
  - Parking, camera, backup, millimeter wave sensor, etc
- Actuators
  - Power steering, LKA, seat belt motors, etc
- Required additional car battery

The Cart: Pros

- Mobility allows for better testing
  - Millimeter wave sensor needs to ‘see’ objects coming towards it
- Teaches you a bit about how a (primitive) car would be put together
- Learn how parts react with & without proper sensors/actuators
- It’s badass

The Cart: Cons

- Wiring these things is awful
- Car parts do NOT fit go-carts
  - Who would have guessed
- Probably should have bought this: http://www.wired.com/autopia/2014/02/open-source-vehicle/?cid=18110044#slide-id-152661

The Cart: FUN!

Dune buggy Charlie

The Cart: Steering

Speedometer

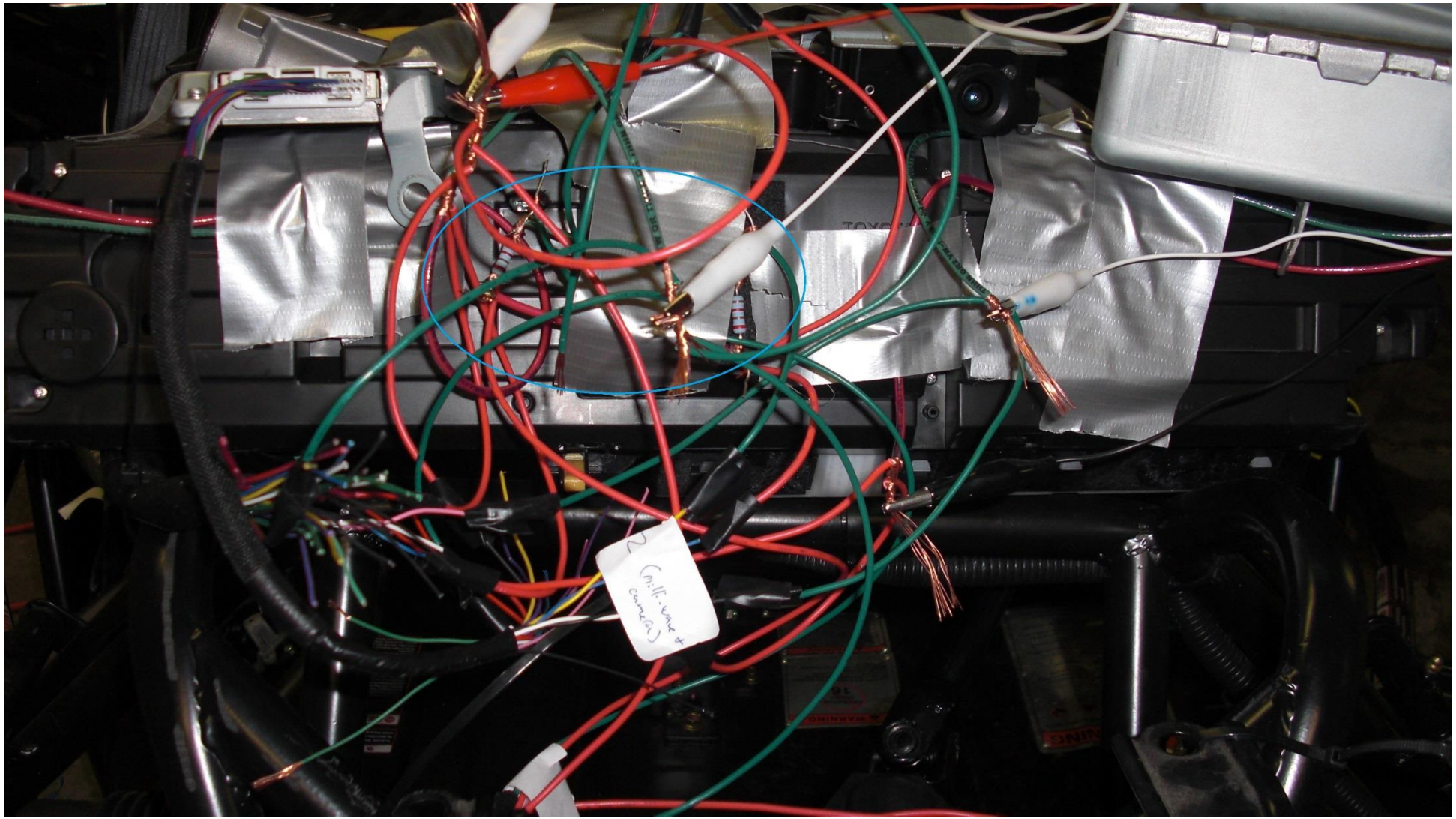
Pitfalls

There are/were many

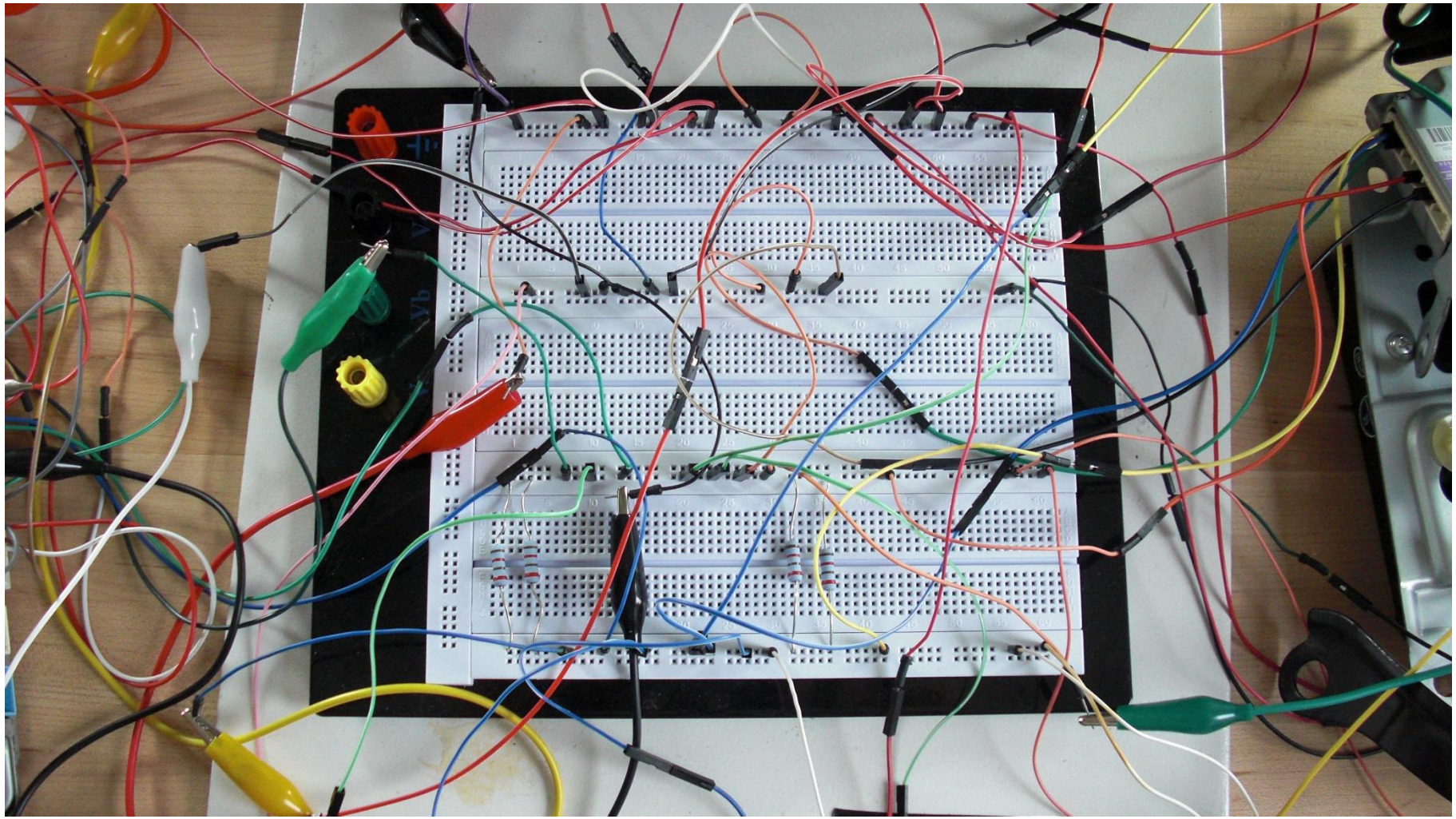
Pitfalls

- Unless re-flashing, don’t get too worried about ‘frying’ an ECU
  - They are quite resilient
- ECUs may send ‘OK’ messages and respond normally to diagnostic requests, but physical attributes may not work
  - We haven’t really figured all this out, but it’s probably due to sensors/actuators/simulated traffic
- Baseline CAN captures can be a problem
- Mechanics accounts are a must
  - Toyota’s was around $1100 USD for a year

Pitfalls: WIRING!

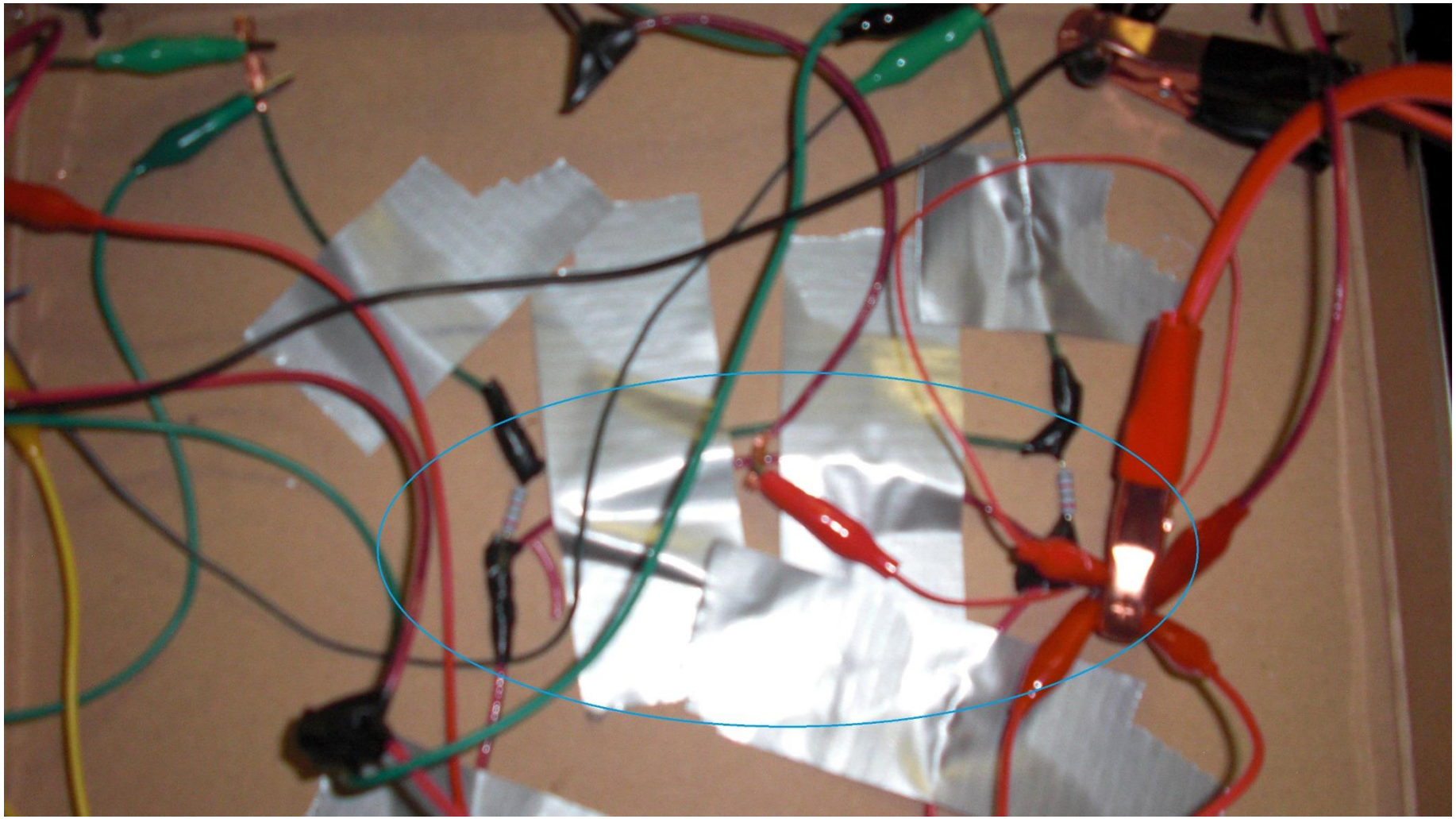


Pitfalls: WIRING!



Debugging…sucks!

Pitfalls: WIRING!



ECU Pricing Examples

- Sometimes you can’t find used ECUs
- USED
  - Prius ECM => ~200 USD
  - Transmission ECU => ~150 USD
  - TPMS ECU => ~50 USD
- New
  - Prius Seatbelt ECU => ~1100 USD

Conclusions

Conclusions

- While not perfect, automotive research can be done without a car
- Cheap, moving alternatives can provide locomotion for a lack of car
- Hopefully this will get even more people involved in autosec
  - Trademark pending
- The government bought us 2 cars and 2 go-carts
  - SUCK IT GRUGQ!

Questions?

Questions?

- Dr. Charlie Miller (@0xcharlie)
  - Twitter Guy
  - cmiller@openrce.org
- Chris Valasek (@nudehaberdasher)
  - Director of Security Intelligence @ IOActive
  - cvalasek@gmail.com