OAK RIDGE National Laboratory

Analysis and Defense of Automotive Networks

Samuel C. Hollifield

Robert A. Bridges, Miki Verma, Michael Iannacone, Dean Deter, Jordan Sosnowski, Kreston Barron, & Frank Combs

Cyber & Applied Data Analytics Division

Oak Ridge National Laboratory

ORNL is managed by UT-Battelle, LLC for the US Department of Energy
This work was supported in part by the U.S. Department of Energy, Office of Science, Office of Workforce Development for Teachers and Scientists (WDTS) under the Science Undergraduate Laboratory Internship program

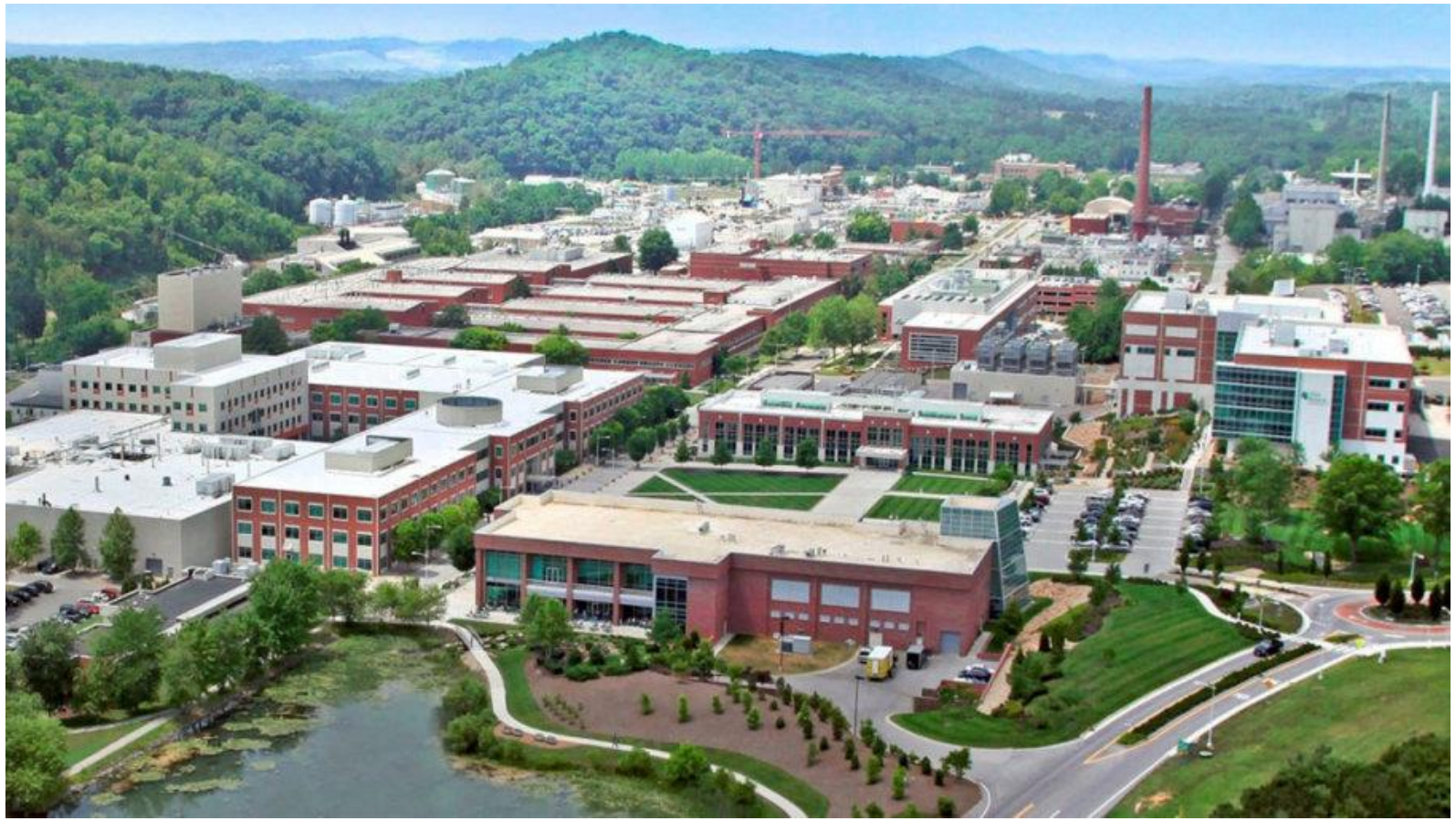
OAK RIDGE INSTITUTE FOR SCIENCE AND EDUCATION

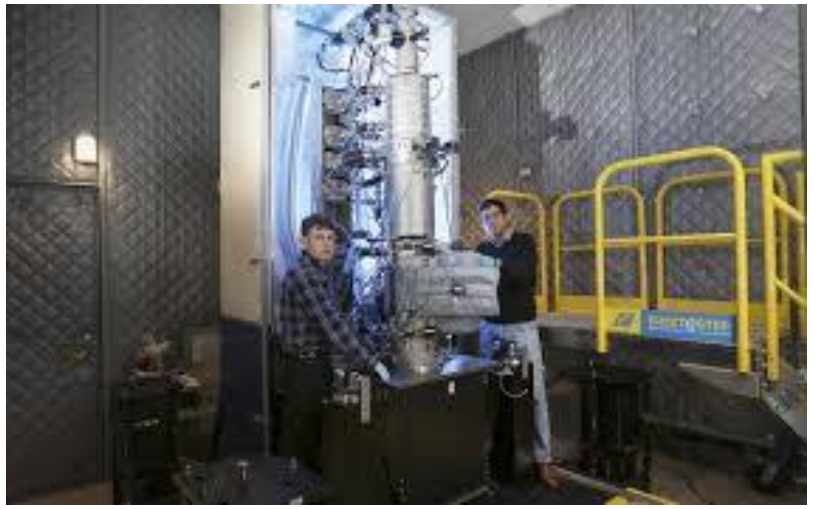
U.S. DEPARTMENT OF ENERGY

Life at a National Lab:

OAK RIDGE National Laboratory

Life at a National Lab (today):





National Laboratories vs. Academia

- **Academia** = Guardians of knowledge
  - Teach it
  - Discover it
  - Preserve it
- **National Laboratories** = Solve the nation's problems
  - From basic research to applications

What exactly is a Controller Area Network? (CAN)

Allows communication between electronic control units (ECUs).

Open, broadcast bus network where every node can read any message.

No way to verify sender integrity.

Very easy to identify and connect to.

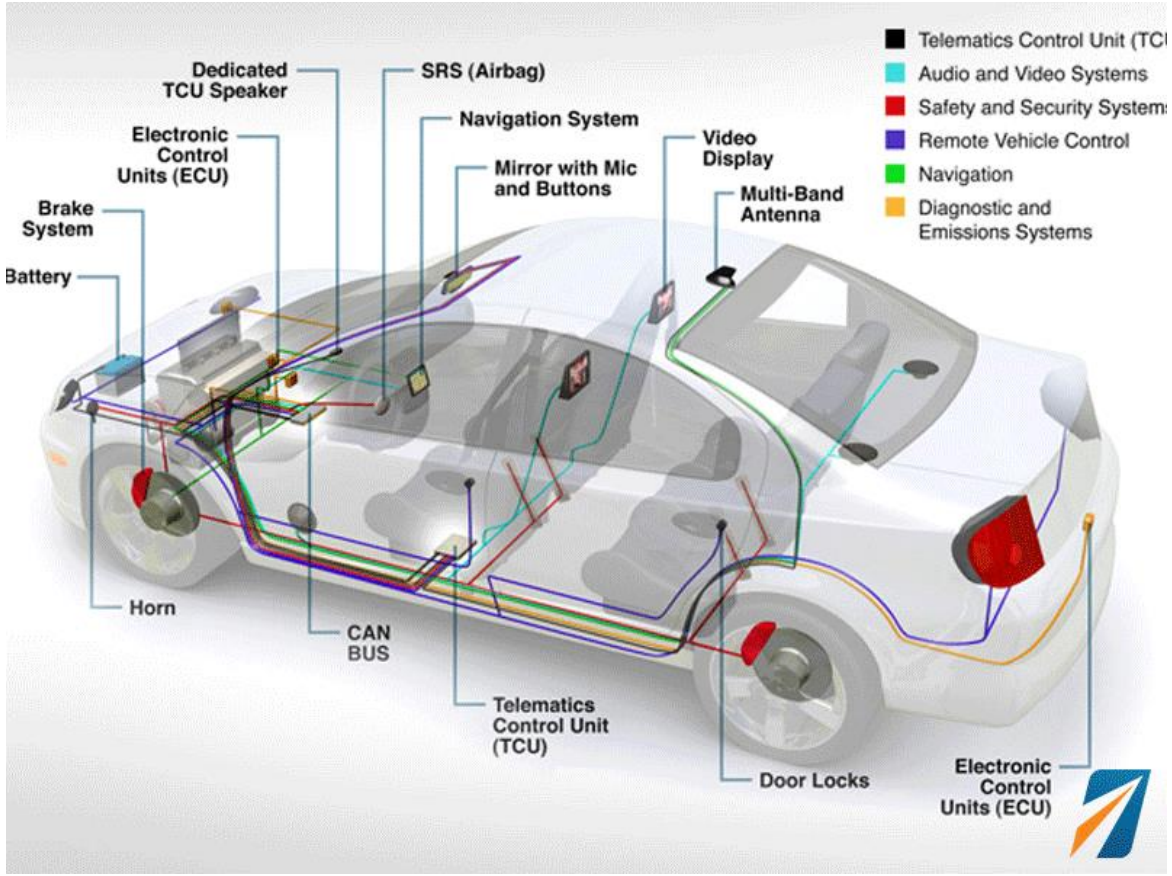
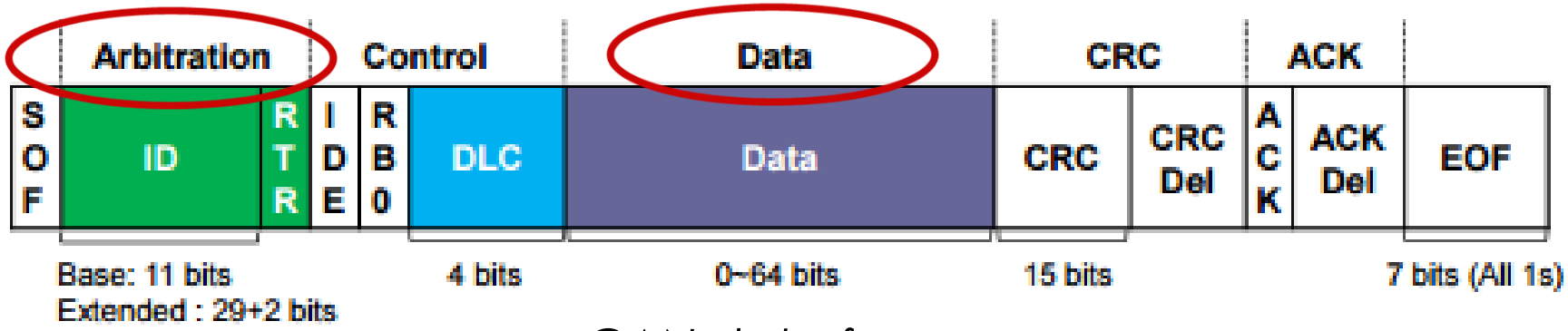


Photo credit: www.fleetistics.com/wp-content/uploads/2016/11/Telematics-Vehicle-Network-System.png

Controller Area Network (CAN)

- CAN Data Frame format:
  - Arbitration ID (AID): indicating priority and indexing contents
  - Data field (or message): containing up to 8 bytes of data



CAN data frame

Photo credit: Cho & Shin, *CCS 2016*

CAN data example

Timestamp AID # data (in hex)

```
(1536160252.263295) can0 223#002000000000004D
(1536160252.263296) can0 3B7#0000000000000000
(1536160252.263296) can0 2C1#0800E2007DC700F9
(1536160252.265273) can0 2D0#06F6010070000047
(1536160252.268251) can0 020#000007
(1536160252.269250) can0 0B4#0000000054000010
(1536160252.269252) can0 024#01FE020762007F15
(1536160252.269252) can0 025#0FEE00178787893
(1536160252.270291) can0 2C4#038D001F0080615E
(1536160252.271312) can0 262#0000000069
(1536160252.271313) can0 4DC#1D00010700000000
```

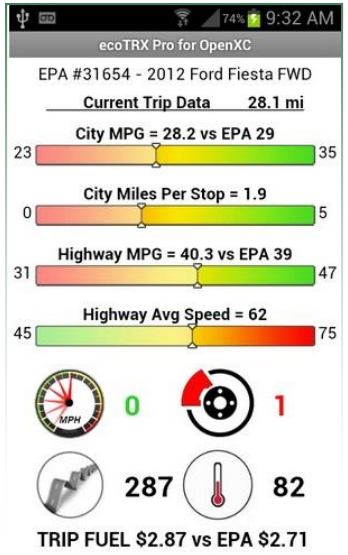
Motivation for Understanding Automotive CAN Data

Intrusion Detection Systems (IDS)

Hackers Miller & Valasek Remotely Kill Jeep Cherokee on Highway (2015)

Photo Credit:
www.cnbc.com/video/2015/07/22/hackers-hijack-moving-jeep-shocking-video.html

After-Market Understanding



ecoTRX™ Pro for OpenXC Personalized MPG App

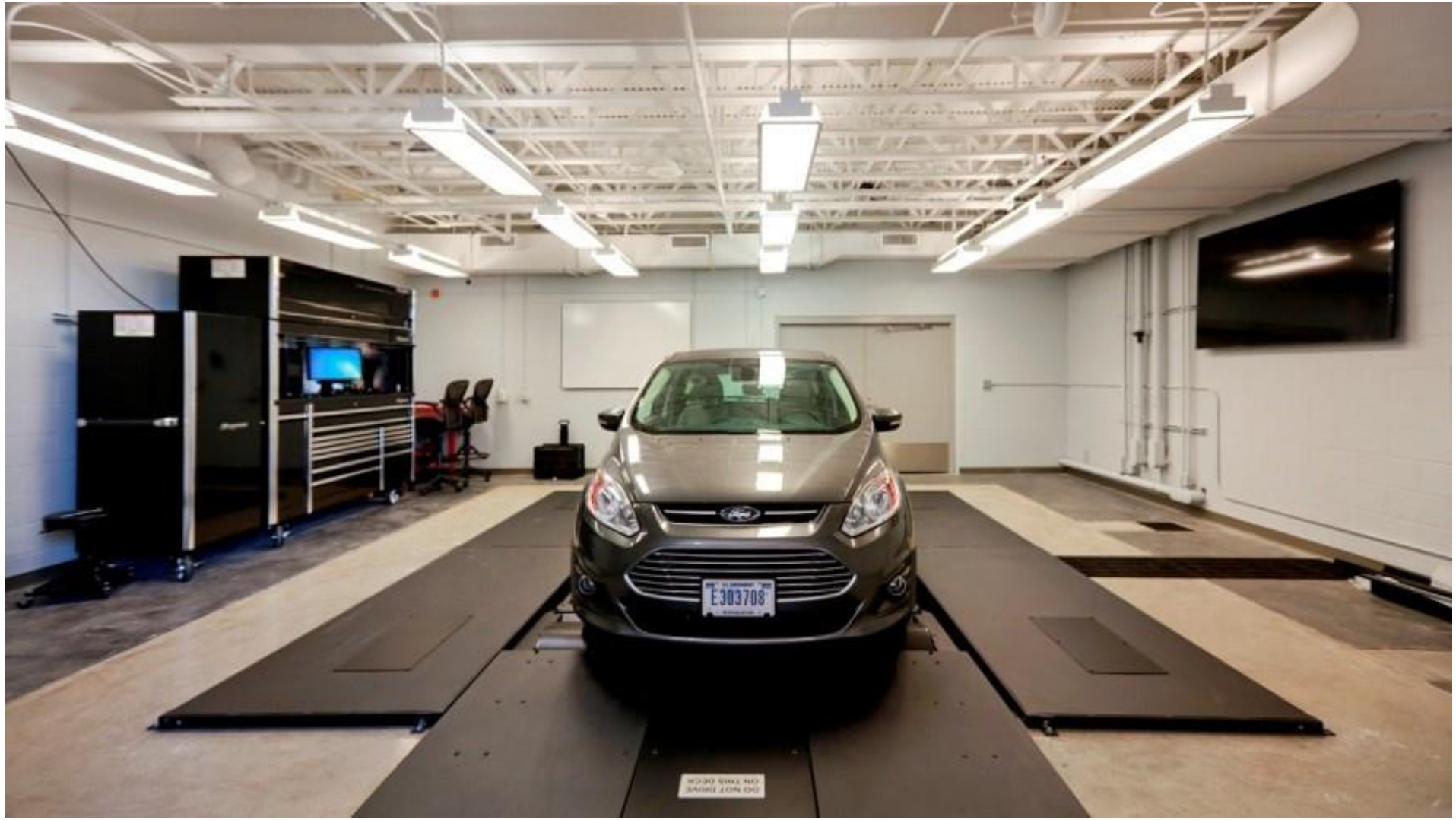
Photo Credit:
devpost.com/software/ecotrx-pro-for-openxc-personalized-mpg-app

Performance Tuning

AEM Fuel/Ignition Controller: Piggyback engine control for boosted racecars

Photo Credit:
www.aemelectronics.com/products/programmable-engine-management-systems/fuel-ignition-controller/fic-6

ORNL's Vehicle Security Laboratory

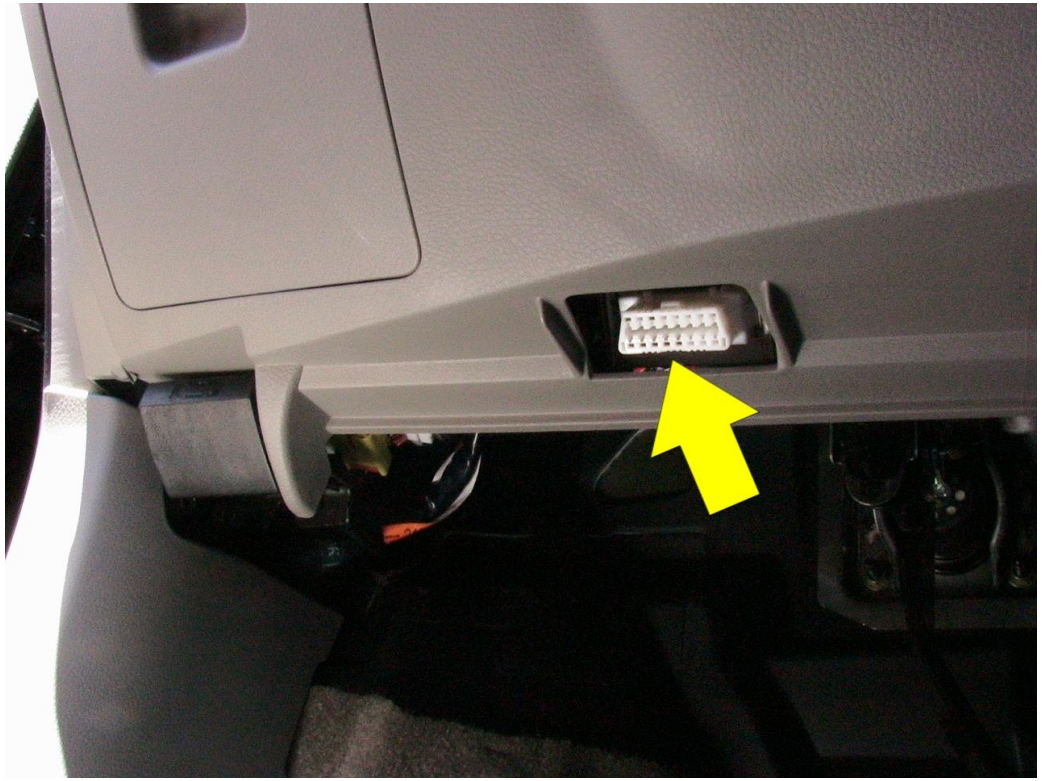


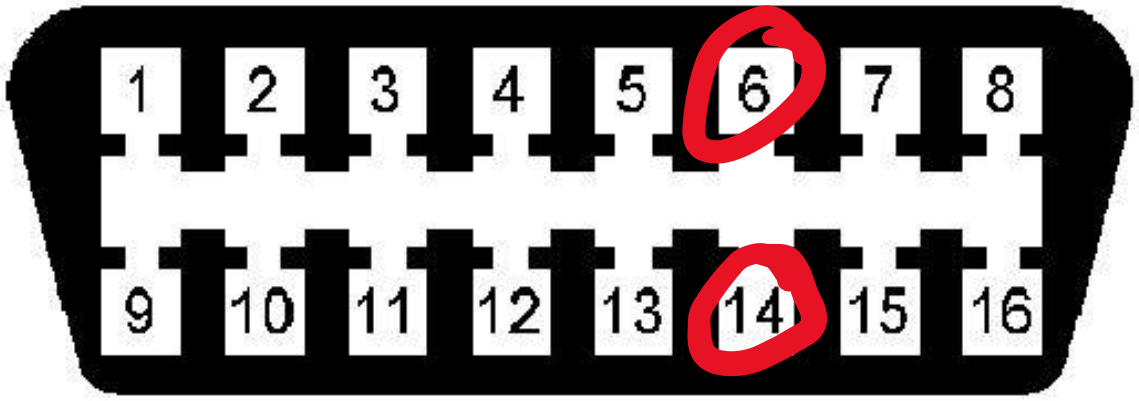
Car's vulnerable?!

Example of what you can do with

- $75 hardware
- Nearly no knowledge
- (and a modern car)

Accessing an Automotive CAN

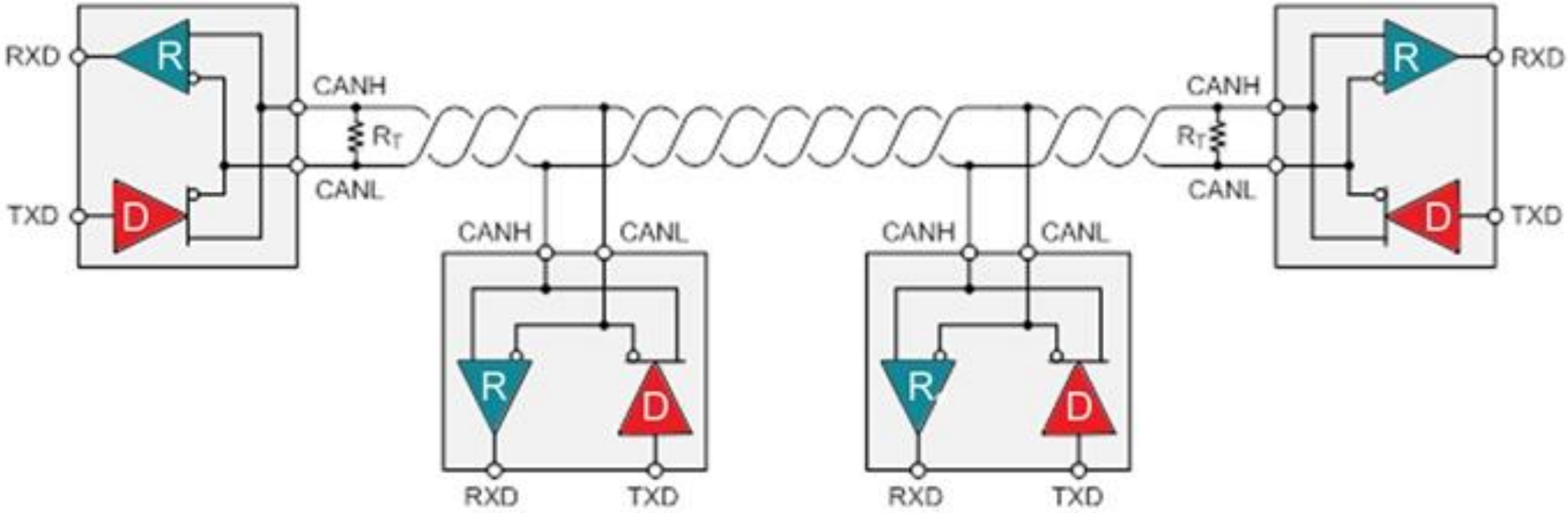




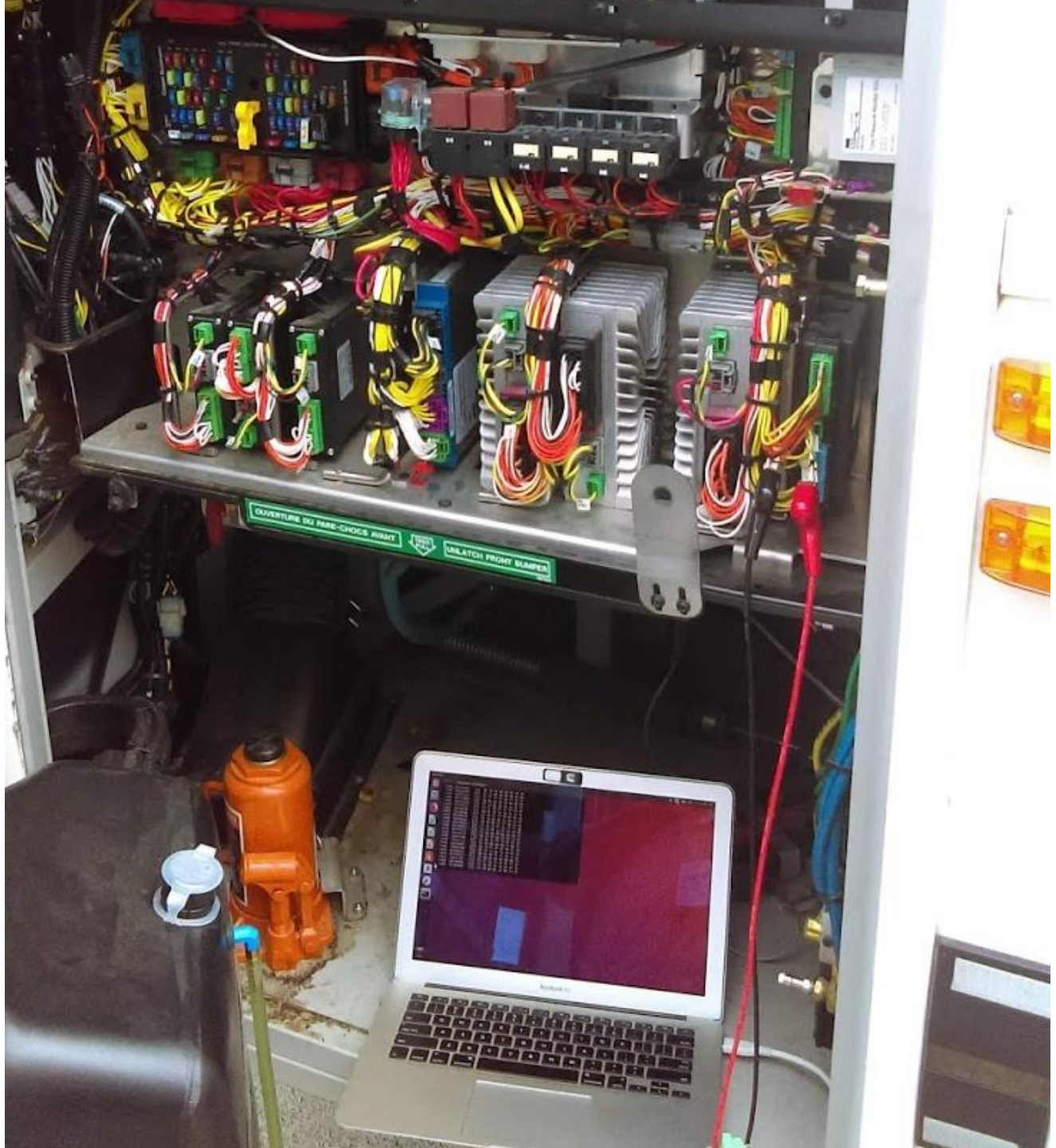
PIN	DESCRIPTION	PIN	DESCRIPTION
1	Vendor Option	9	Vendor Option
2	J1850 Bus +	10	j1850 BUS
3	Vendor Option	11	Vendor Option
4	Chassis Ground	12	Vendor Option
5	Signal Ground	13	Vendor Option
6	CAN (J-2234) High	14	CAN (J-2234) Low
7	ISO 9141-2 K-Line	15	ISO 9141-2 Low
8	Vendor Option	16	Battery Power

OBD-II Connector and Pinout

Accessing an Automotive CAN




PREVOST
10000


OUVERTURE DU PARE-CHOCS AVANT
UNLATCH FRONT BUMPER

OAK RIDGE National Laboratory

Building Hardware for CAN Analysis

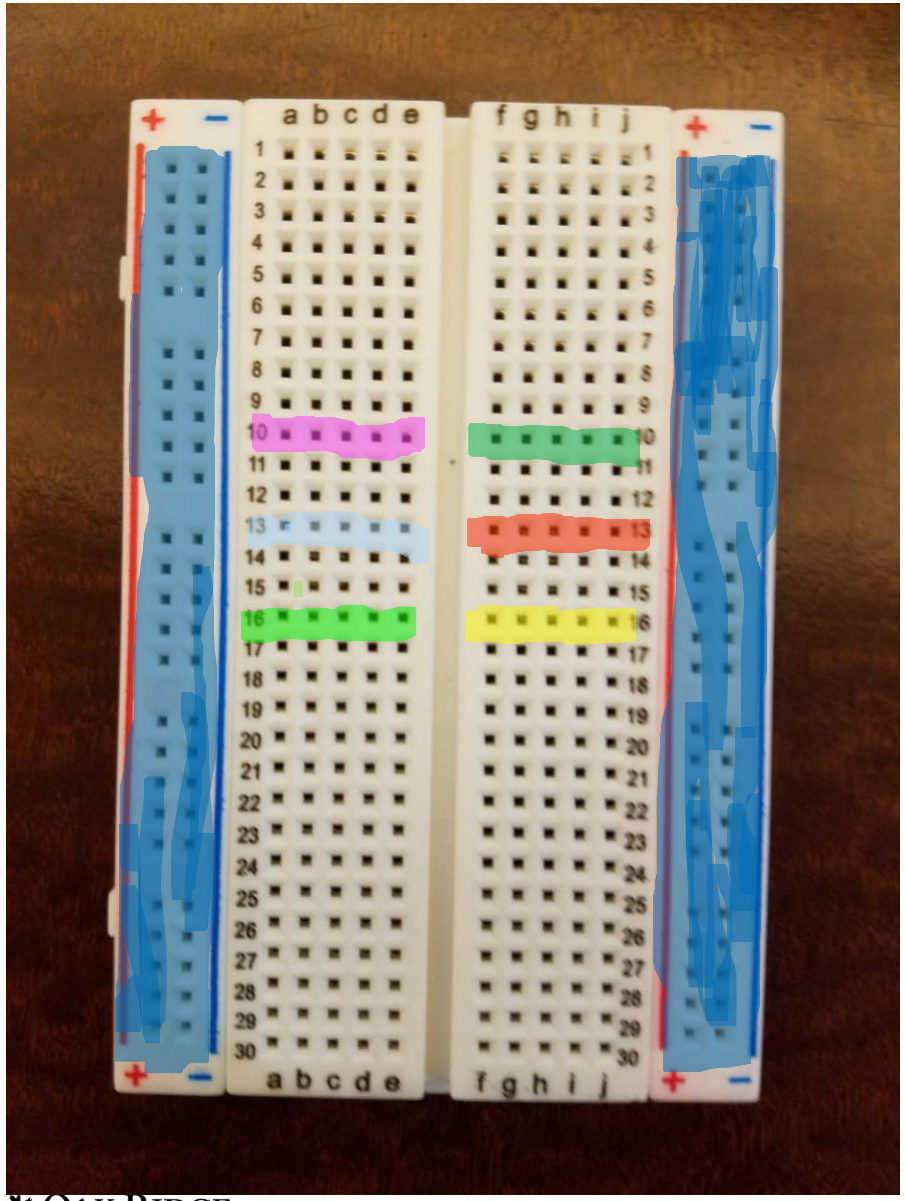
Prerequisite Hardware for CAN Communication:

- Microcontroller or computer
- CAN transceiver
- CAN controller
- Another node on the network

Exact Hardware Provided Today:

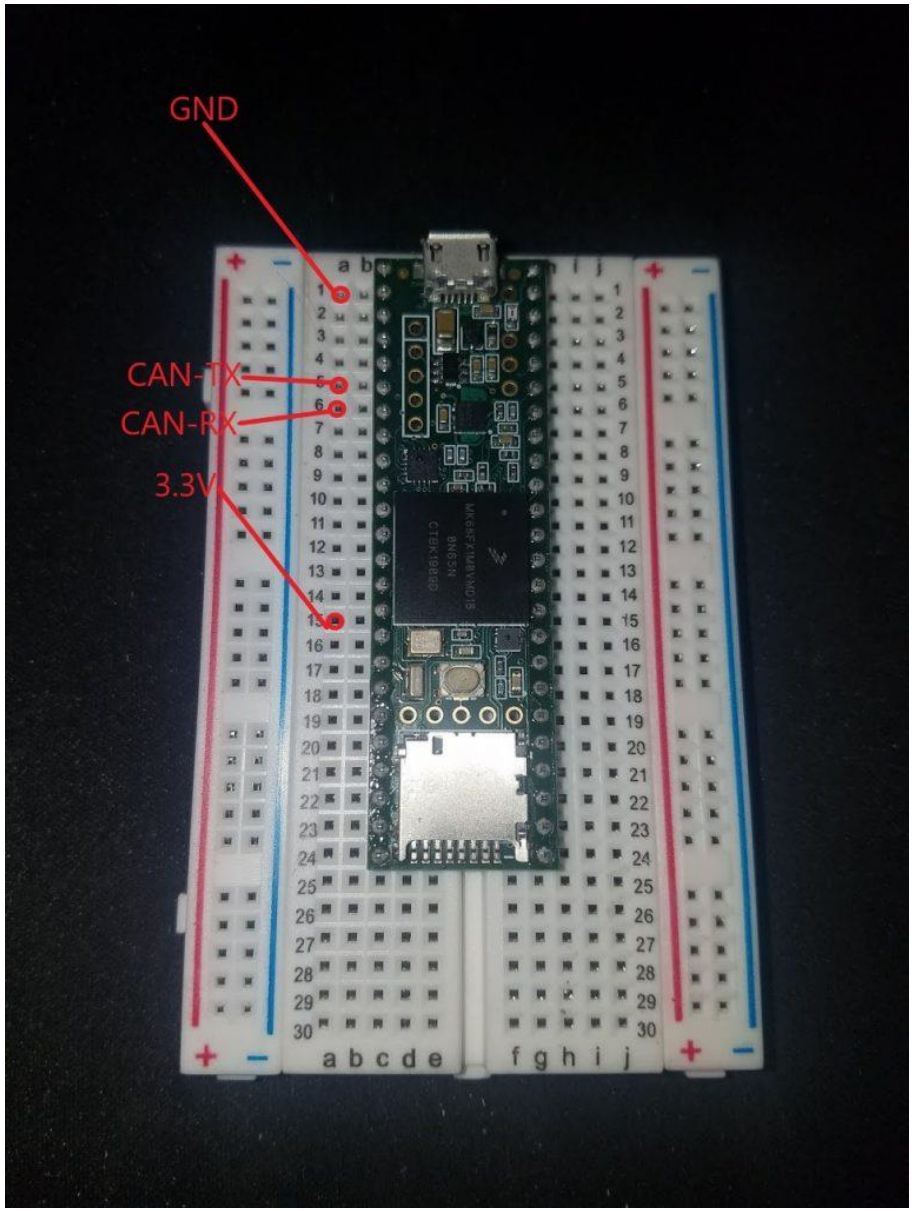
- Teensy3.6
- Waveshare SN65HVD230 CAN Transceiver Board
- OBD-II Cable
- USB to micro-USB Cable
- Breadboard
- Assorted wires, GPIO cables

Quick Note: How to Breadboard

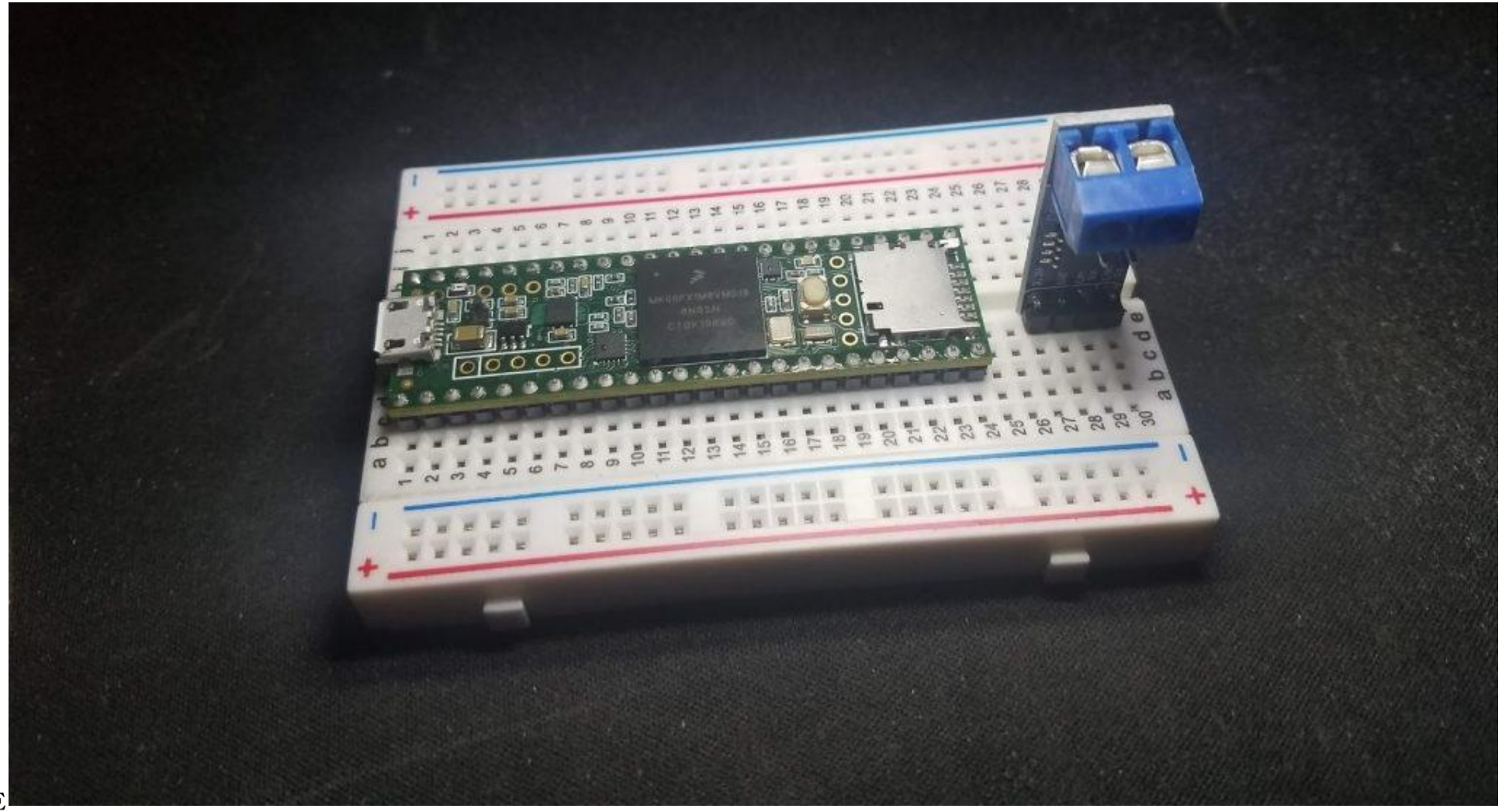


- Breadboard is typically oriented so columns and rows are easily readable.
- Middle columns are labeled **a** through **j**. There is no circuit vertically.
- Middle rows are labeled **1** through **30**. A circuit exists on each row, separated in half by the breadboard.
- Outer columns are labeled **+** and **–**. A circuit exists the entire length of each column. A circuit does not exist horizontally.

Step 1: Place the Teensy in the breadboard. USB side on Row # 1

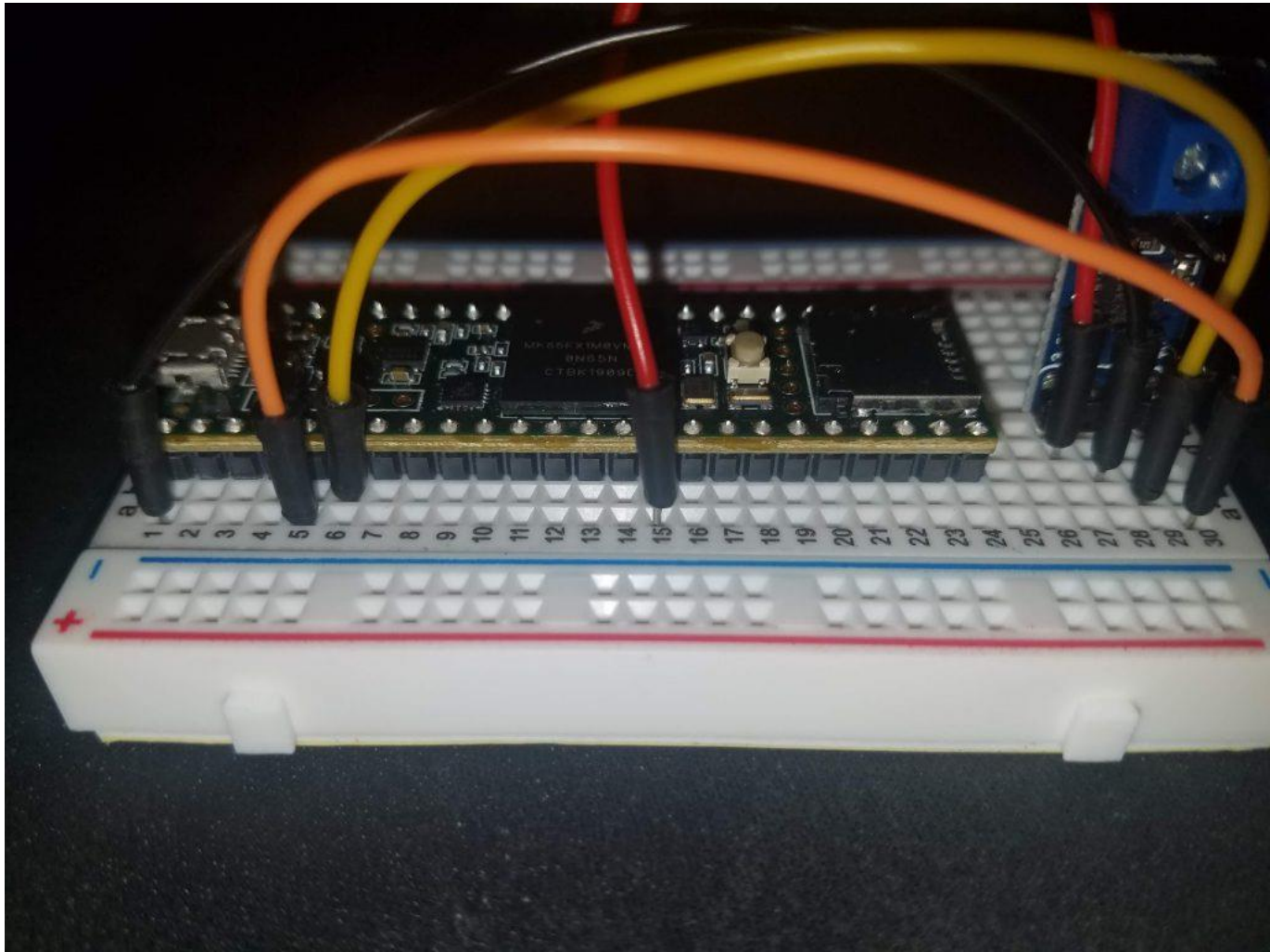


Step 2: Insert the Waveshare CAN Transceiver in rows #27-30, with CAN-TX in row #30



Step 3: Connect the appropriate wires from the Teensy3.6 to the CAN Transceiver

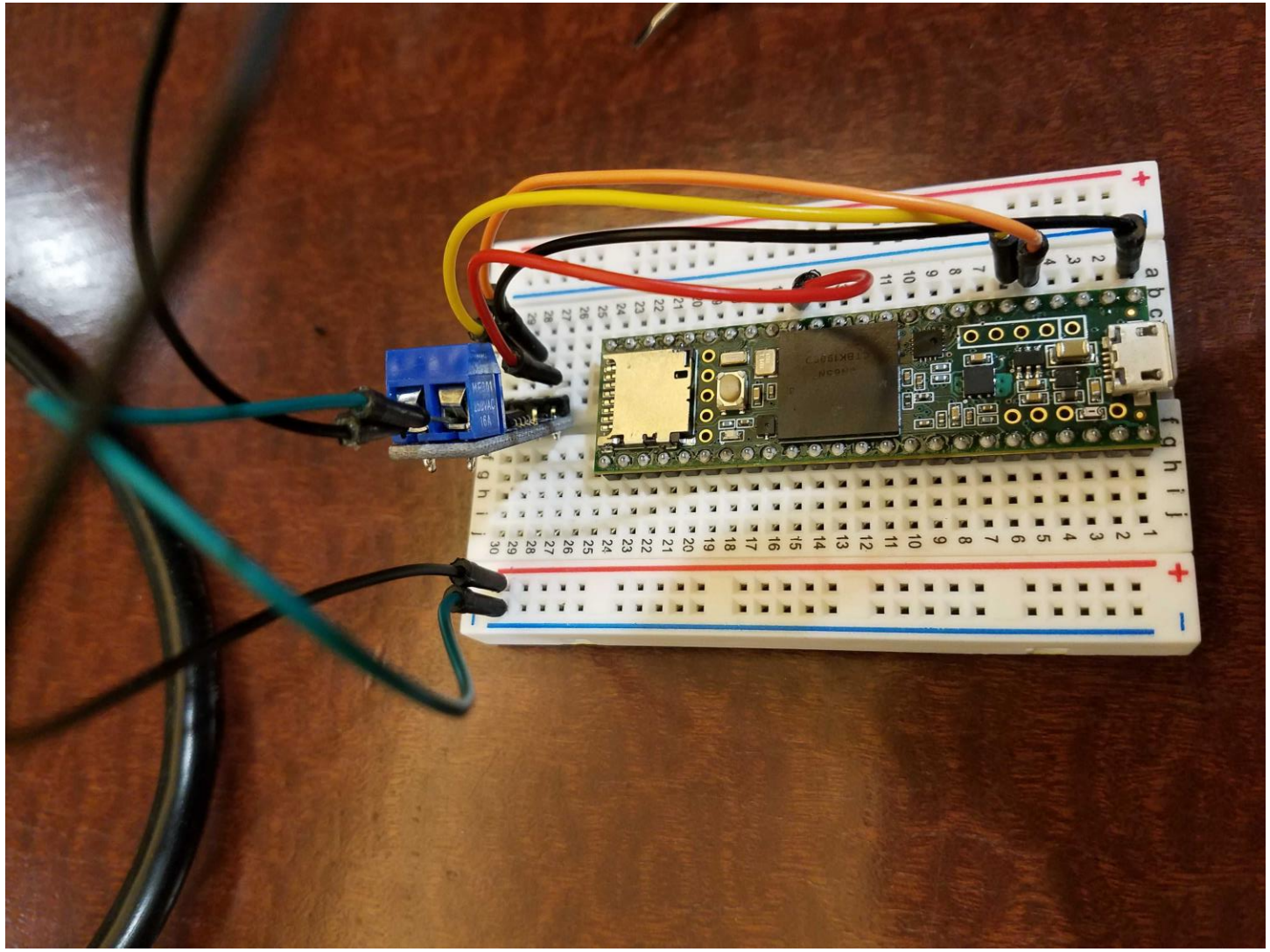
- Pin 1 -> Pin 28 (GND)
- Pin 5 -> Pin 30 (CAN TX)
- Pin 6 -> Pin 29 (CAN RX)
- Pin 15 -> Pin 27 (3v3 Power)



Connect the CAN Transceiver to the + and – rails on your breadboard.

CANH is +
CANL is –

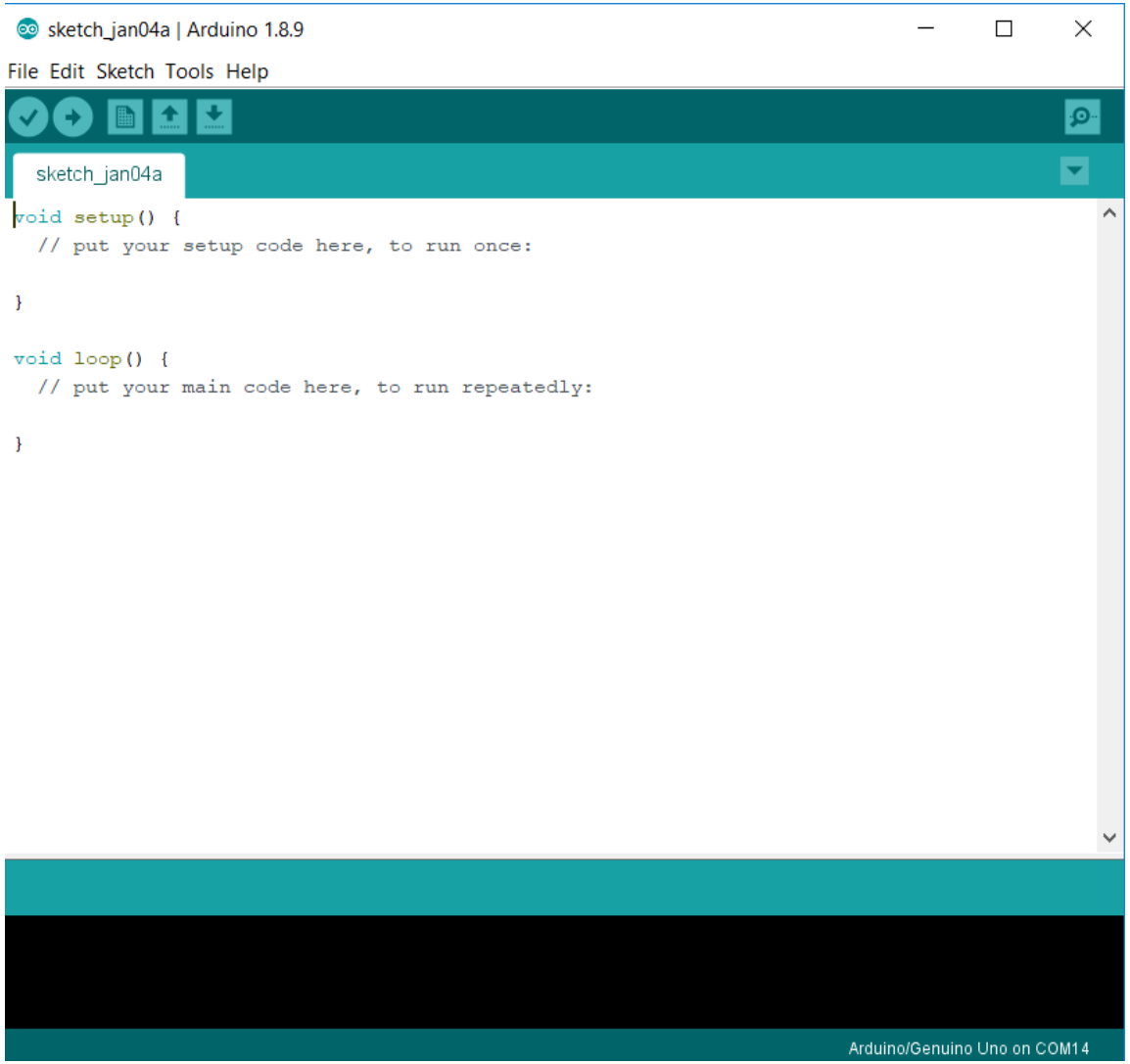
Find a neighbor, and use wires to connect your CAN using breadboards.



OAK RIDGE National Laboratory

Sending and Receiving CAN Messages

Step 1: Fire up the Arduino IDE…



…and follow along!

OAK RIDGE National Laboratory

Team up with someone else who has a Teensy to send & receive message to the serial console

OAK RIDGE National Laboratory

Interacting with a Vehicle (or a Raspberry Pi)

WARNING: IT CAN BE DANGEROUS (as seen earlier) TO INJECT OR EVEN PLUG INTO THE OBD PORT OF YOUR CAR! USE CAUTION AND NEVER DO IT WHILE DRIVING.

…and follow along!

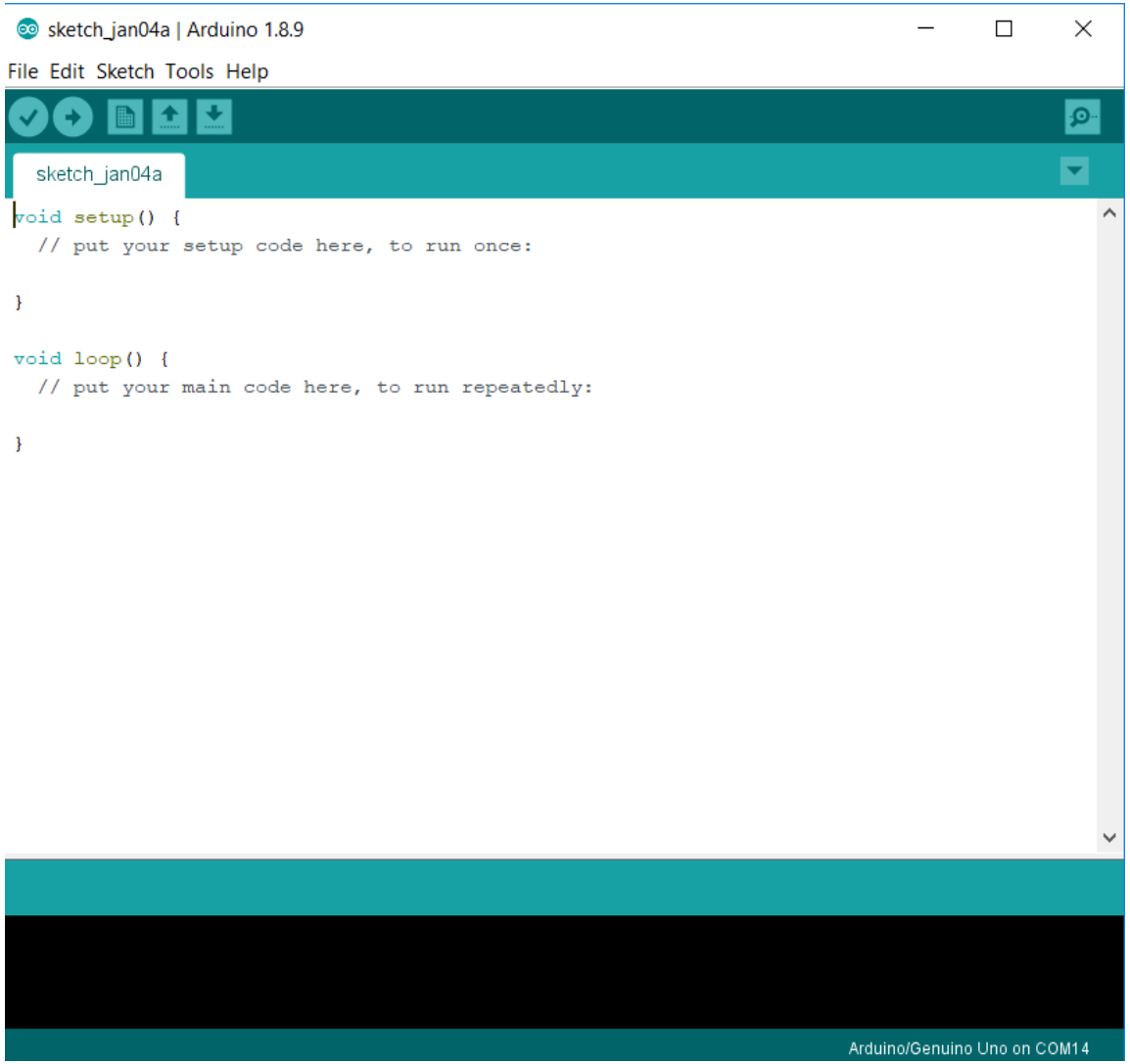
Important Things to Know Before Connecting to Vehicles

- Two nodes must on the network to transmit (a receiving node must exist to acknowledge a message)
- Each vehicle has a preset bitrate (speed) of communication for the CAN. This is usually 500kbps. Choosing the wrong bitrate can cause network interruption.
- CAN is meant to be terminated. If communication doesn't occur, add a 120-ohm resistor between CANH & CANL

Things to keep in mind when interpreting data

- One ECU will have **many** Arbitration IDs
- Each vehicle (make/model/trim) will likely have a unique CAN
- OEMs keep the translations for the network hidden and obfuscated
- More than one CAN may exist on a vehicle

Step 1: Fire up the Arduino IDE…



…and follow along!

Decoding CAN Data to Find Useful Signals

- Sort of difficult to do with the Teensy alone.
- SavvyCAN can certainly help pinpoint and arrange messages.
- Simply, a Linux tool called '*can-utils*' can help identify changing bits immensely
- Save output from Teensy—open Linux & replay data into *can-utils*

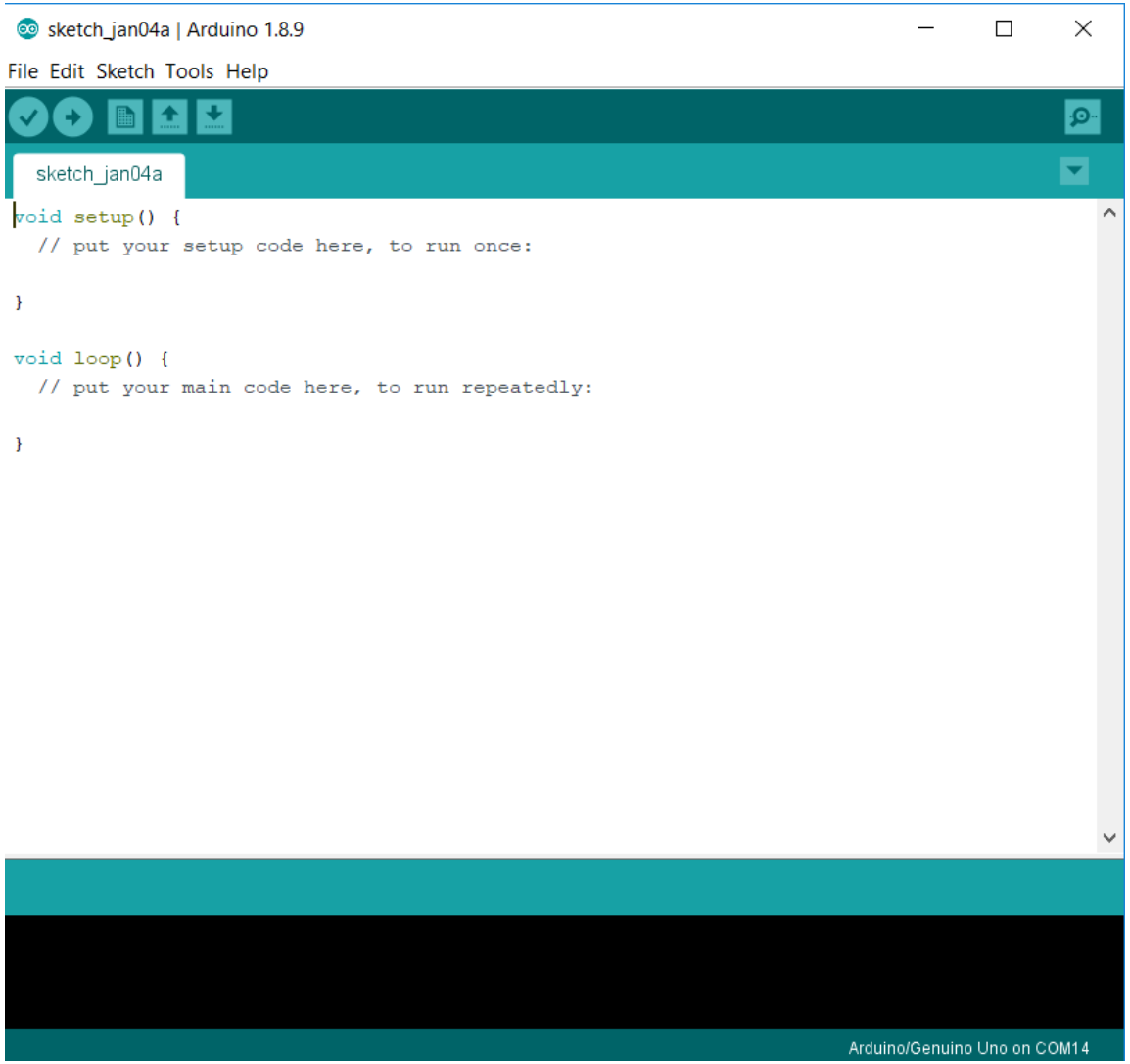
OAK RIDGE National Laboratory

Timing-Based Detection of Automotive Cyberattacks

Timing-Based Detection of Automotive Cyberattacks

- CAN frames are sent at regular intervals for each Arbitration ID (and often redundant data)
- Simplest attack involves injecting frames on the bus
- Must be sent at least as fast as ambient message for physical effect
- We can detect such attacks by modeling inter-frame arrival times (Gmiden et al., 2016, Song et al., 2016, Moore et al., 2017)

Step 1: Fire up the Arduino IDE…



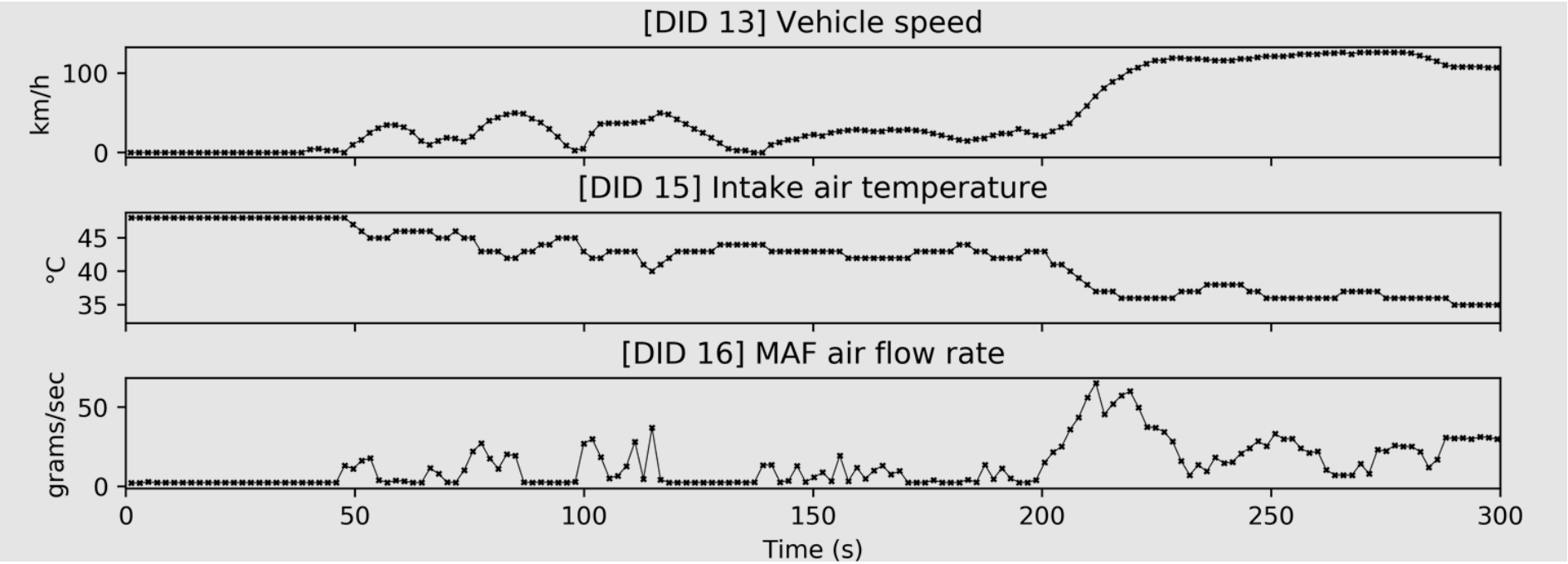
…and follow along!

OAK RIDGE National Laboratory

On-Board Diagnostics (OBD-II)

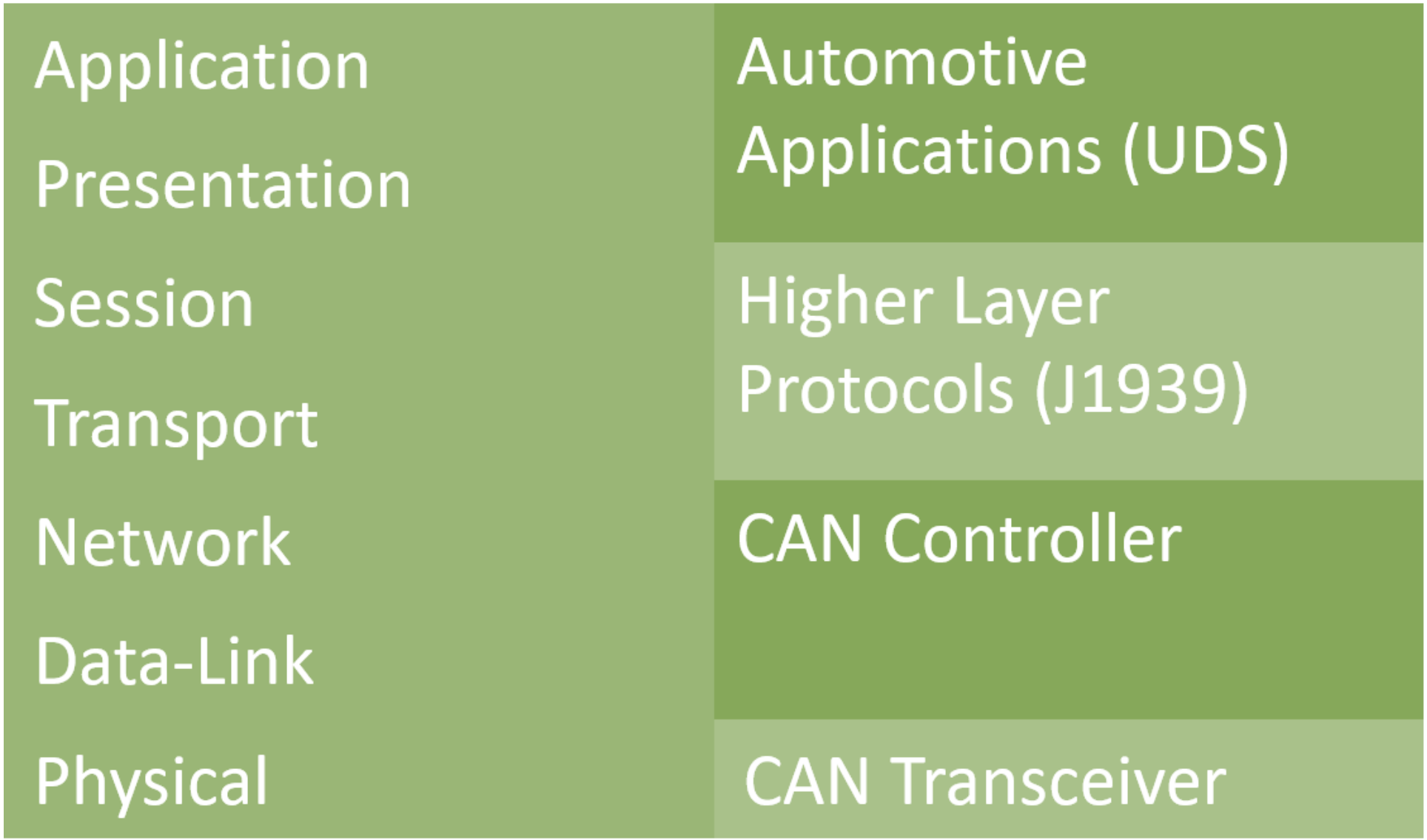
Diagnostic Data

- OEMs, mechanics, service stations, emission tests, and more rely on a standardized set of diagnostic responses inside of CAN



Three diagnostic signals (DIDs 13, 15, 16) queried at a rate of .6Hz over 5 minutes

How does On-Board Diagnostics fit with CAN?



Retrieving Diagnostics from Vehicles

- Wikipedia is our friend! (https://en.wikipedia.org/wiki/OBD-II_PIDs)
- First, we must send a request for the specific data we want
- Diagnostic broadcasts are sent on Arbitration ID 0x7DF. Replies are given by multiple ECUs.
- Then, we must parse the response given some standard message structure

Using On-Board Diagnostics via CAN

- List of Service IDs in hex

Service (hex)	Description
01	Show current data
02	Show freeze frame data
03	Show stored Diagnostic Trouble Codes
04	Clear Diagnostic Trouble Codes and stored values
05	Test results, oxygen sensor monitoring (non CAN only)
06	Test results, other component/system monitoring (Test results, oxygen sensor monitoring for CAN only)
07	Show pending Diagnostic Trouble Codes (detected during current or last driving cycle)
08	Control operation of on-board component/system
09	Request vehicle information
0A	Permanent Diagnostic Trouble Codes (DTCs) (Cleared DTCs)

PID (hex)	PID (Dec)	Data bytes returned	Description
00	0	4	PIDs supported [01 - 20]
01	1	4	Monitor status since DTCs cleared. (Includes malfunction indicator lamp (MIL) status and number of DTCs.)
02	2	2	Freeze DTC
03	3	2	Fuel system status
04	4	1	Calculated engine load
05	5	1	Engine coolant temperature
06	6	1	Short term fuel trim—Bank 1
07	7	1	Long term fuel trim—Bank 1
08	8	1	Short term fuel trim—Bank 2
09	9	1	Long term fuel trim—Bank 2
0A	10	1	Fuel pressure (gauge pressure)
0B	11	1	Intake manifold absolute pressure
0C	12	2	Engine RPM
0D	13	1	Vehicle speed
0E	14	1	Timing advance
0F	15	1	Intake air temperature
10	16	2	MAF air flow rate
11	17	1	Throttle position
12	18	1	Commanded secondary air status
13	19	1	Oxygen sensors present (in 2 banks)

Using On-Board Diagnostics

- Over 150 possible Parameter IDs
- Each car will vary. We can query for supported PIDs using 00 & every 0x32 PID after.
- Very useful for diagnosing automotive faults, clearing check-engine lights, and generating ground truth for signal matching.

Example Send/Receive Available OBD Messages

7DF	#	02	01	00	00	00	00	00	00
AID		Length	Serv. ID	PID	Padding	Padding	Padding	Padding	Padding

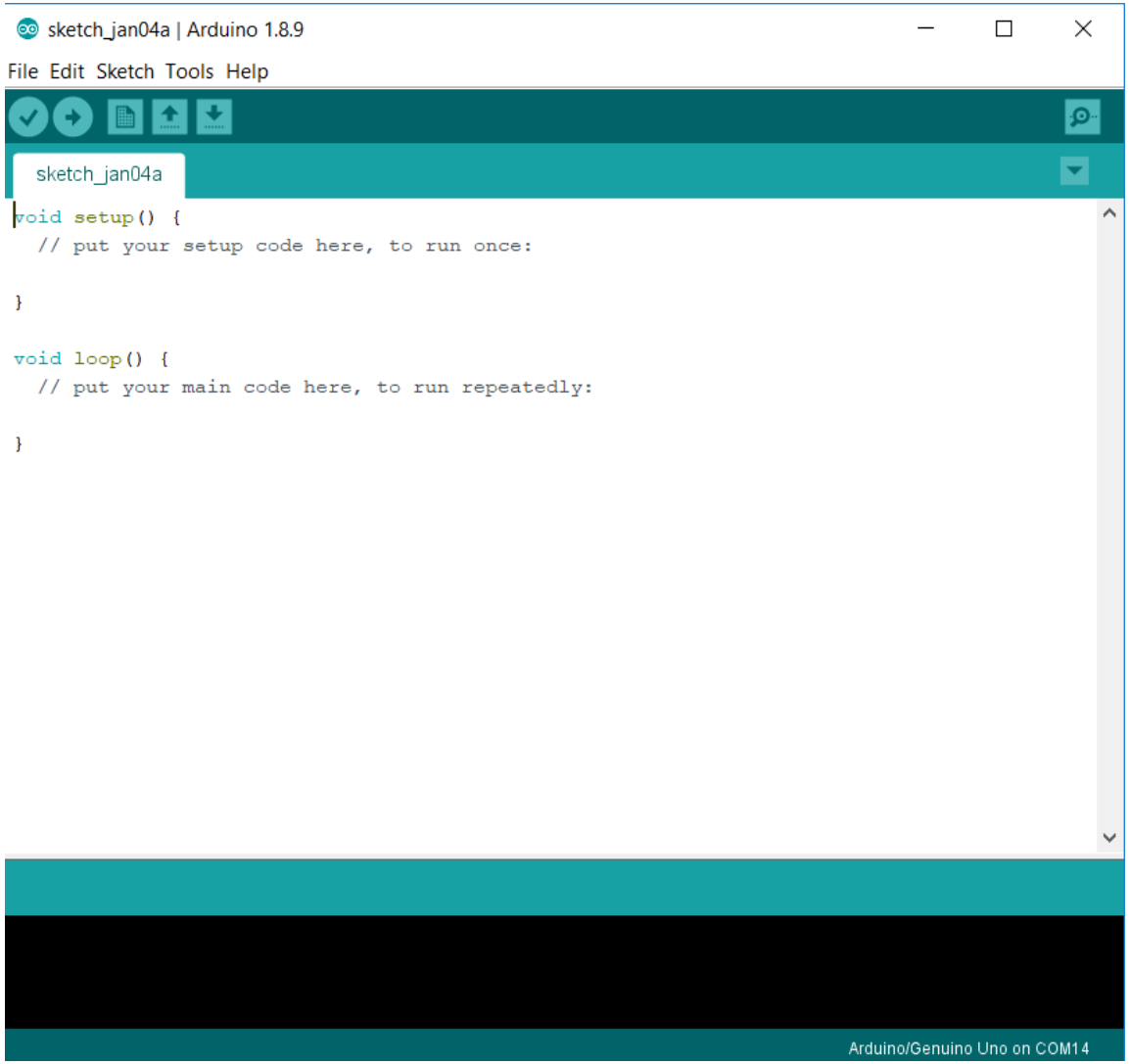
7E8	#	06	41	00	BE	1F	A8	13	00
AID		Length	Serv. ID + 40	PID	Data	Data	Data	Data	Padding

What does it mean?

Hexadecimal	B				E				1				F				A				8				1				3			
Binary	1	0	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	0	1	0	1	0	0	0	0	0	0	1	0	0	1	1
Supported?	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	No	No	No	No	No	No	Yes	No	No	Yes	Yes
PID number	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	20

Automating Diagnostic Queries

Step 1: Fire up the Arduino IDE…



…and follow along!

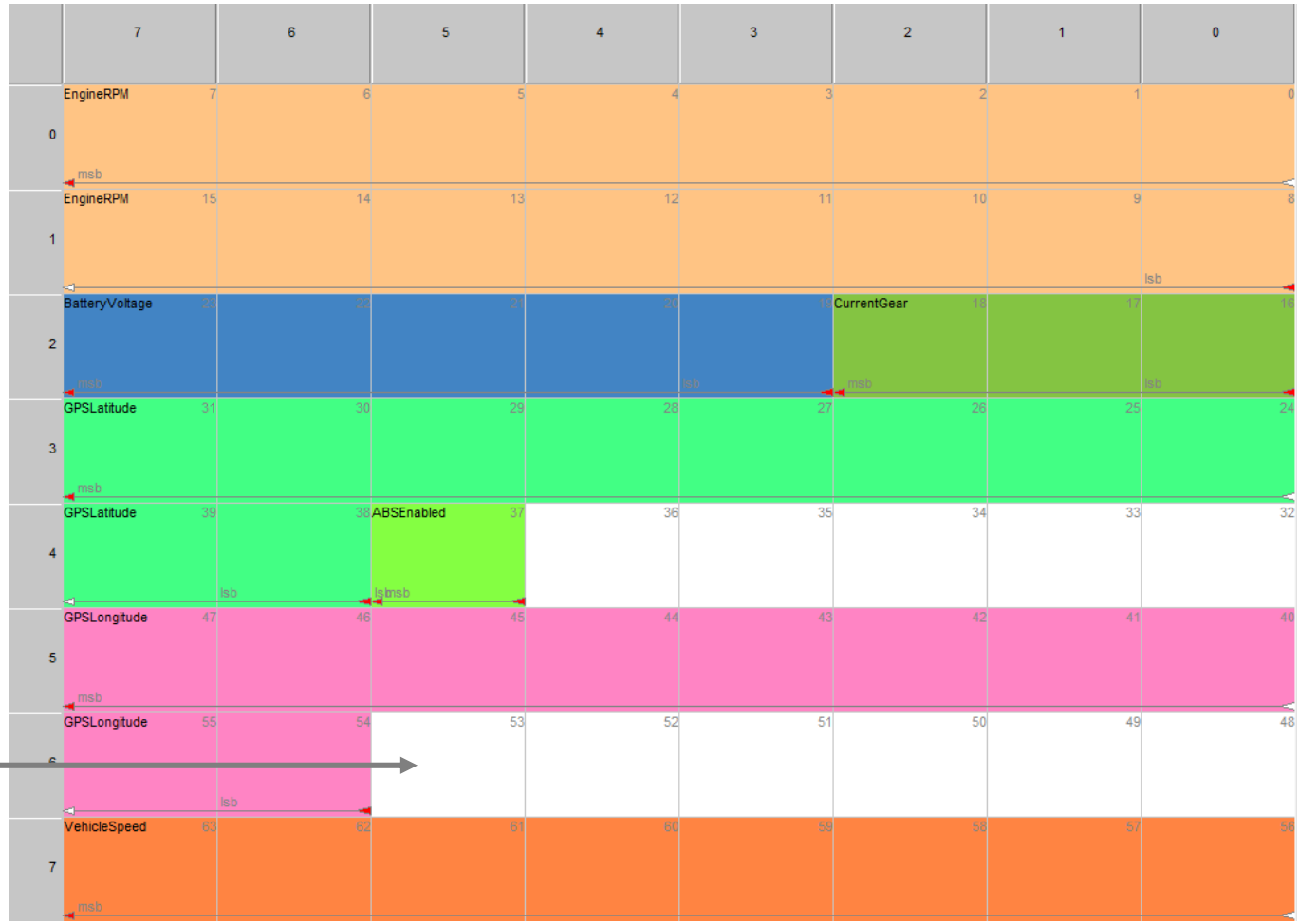
OAK RIDGE National Laboratory

Automatic Discovery of CAN Message Encodings

Tokenization and Translation Problem

CAN Signal: Bytes 1-2 Engine RPM

Unused Bit

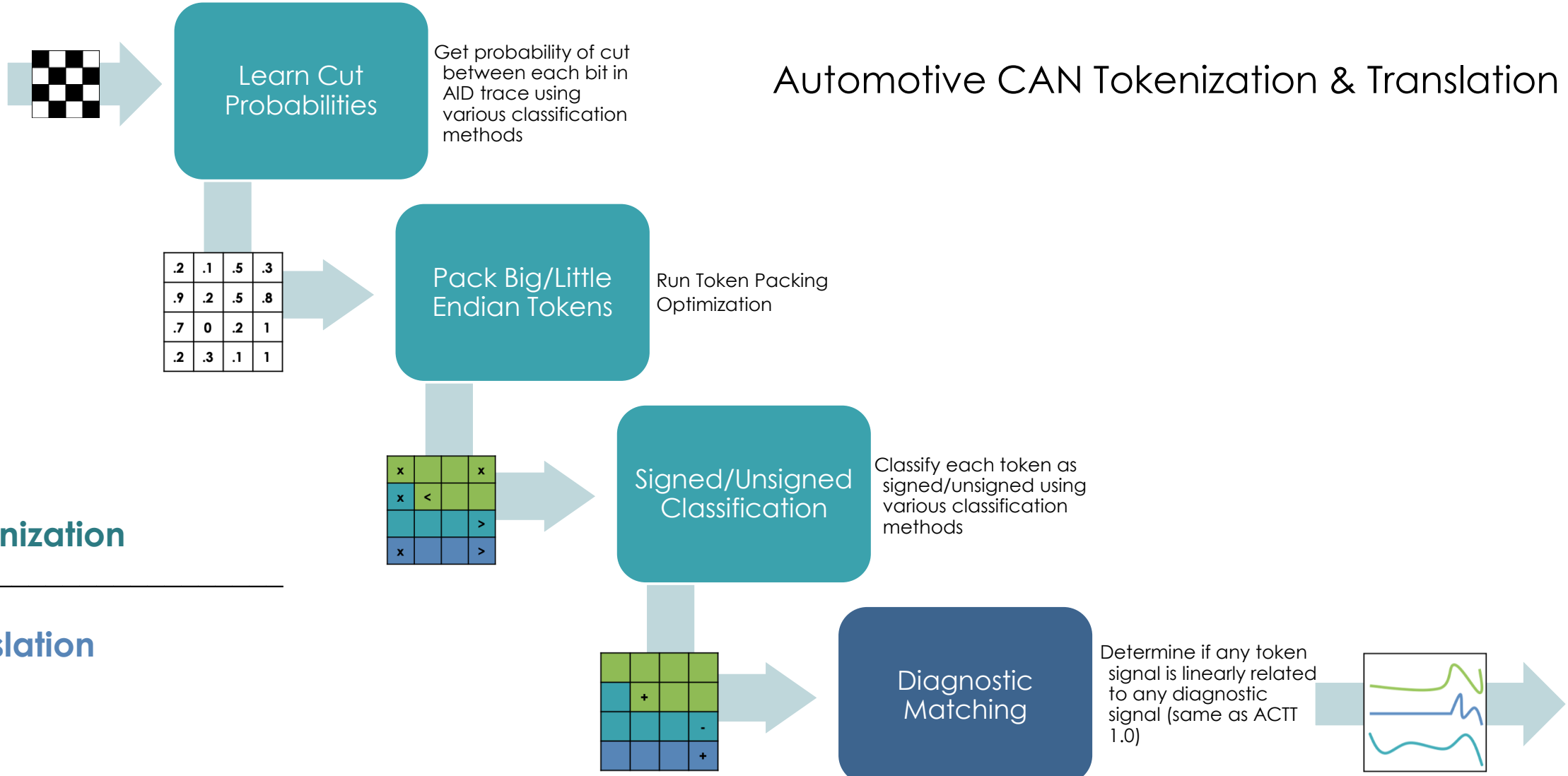


64-bit CAN data field description defined in DBC: CAN signals (color), unused bits (white)

Photo Credit: hackaday.com/2013/10/22/can-hacking-the-in-vehicle-network/

ACTT 2.0 Pipeline

Automotive CAN Tokenization & Translation



Special Offer for CodeMash Attendees:

- Want to automatically find some signals in your own car?
  - If you drove to CodeMash & purchased the Teensy kit (or otherwise can generate data in the can-utils format).
  - Collect data from your car augmented with diagnostic requests
  - Tweet/Slack me (codemash.slack.com) or @Cyrodox and we will coordinate the analysis!

OAK RIDGE National Laboratory

Recap & Wind Down

Recapping Automotive Networks

- We took advantage of the Controller Area Network (CAN) to learn:
  - How to send & receive basic messages
  - How message timing can be used to prototype a basic intrusion detector
  - How to leverage on-board diagnostics to learn about our cars and create new applications
  - That we should never inject random messages while driving, and exercise due care when plugging ANYTHING into our OBD port.

Further Reading:

- Car Hacker's Handbook (FREE!) http://opengarages.org/handbook/
- Kvaser Education on CAN-bus (FREE!) https://www.kvaser.com/can-protocol-tutorial/
- Bosch Automotive Electrics and Automotive Electronics (not free—but very excellent)
- ACTT: Automotive CAN Tokenization & Translation (Shameless plug) https://arxiv.org/abs/1811.07897

OAK RIDGE National Laboratory

Analysis and Defense of Automotive Networks

Samuel C. Hollifield

Robert A. Bridges, Miki Verma, Michael Iannacone, Dean Deter, Jordan Sosnowski, Kreston Barron, & Frank Combs

Cyber & Applied Data Analytics Division

Oak Ridge National Laboratory

ORNL is managed by UT-Battelle, LLC for the US Department of Energy
This work was supported in part by the U.S. Department of Energy, Office of Science, Office of Workforce Development for Teachers and Scientists (WDTS) under the Science Undergraduate Laboratory Internship program

OAK RIDGE INSTITUTE FOR SCIENCE AND EDUCATION

U.S. DEPARTMENT OF ENERGY