

Read-Only Bus Access for ELDs and Other Connected Devices



Presented by Hayden Allen

Mechanical Engineering Undergraduate Student

Advisor: Dr. Jeremy Daily



THE UNIVERSITY *of*
TULSA

Student CyberTruck Experience

Who Am I?



THE UNIVERSITY of
TULSA
Student CyberTruck Experience

- Hayden Allen
 - University of Tulsa
 - Mechanical Engineering '18
 - President of TU Auto Club
 - Automotive Enthusiast
 - Avid Weekend Racer, Weekend Mechanic
 - Currently Building: Miata Kart, 1973 BMW 2002, Duramax '52 3100
 - SAE Cyber Auto Challenge Participant



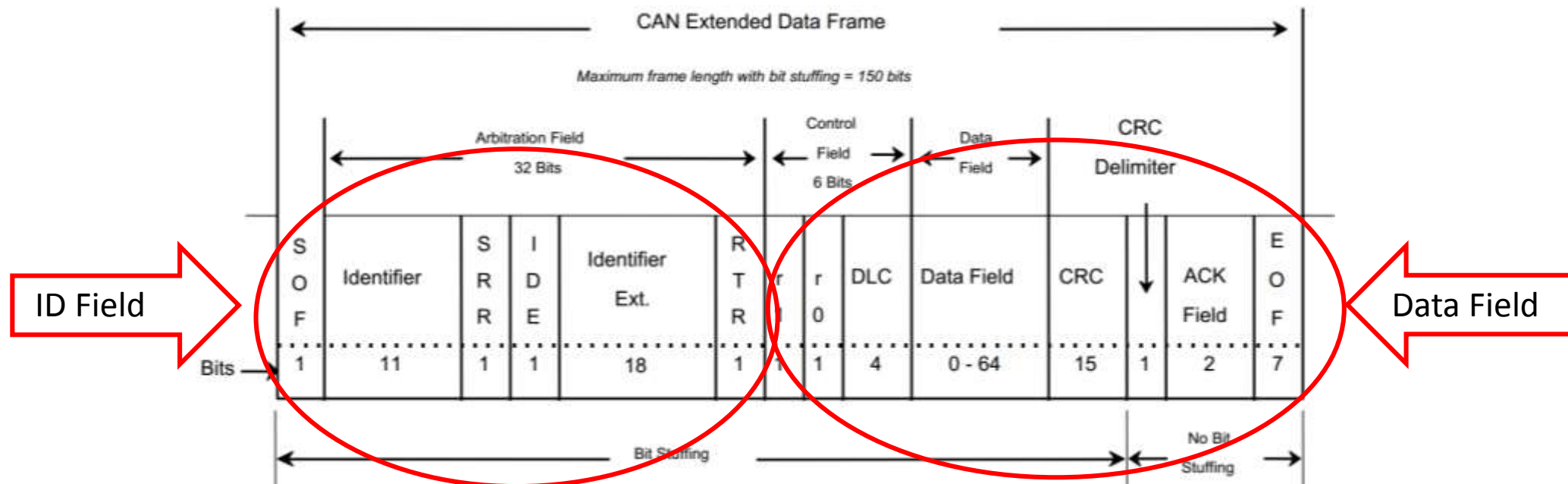
CAN bus

- What is a CAN bus?
 - CAN: Controller Area Network
 - The network that enables most of the electronic control units on the truck to communicate
 - Electronic Brake Controller
 - Engine Control Module
 - Instrument Cluster
 - Body Control Module



How does it work?

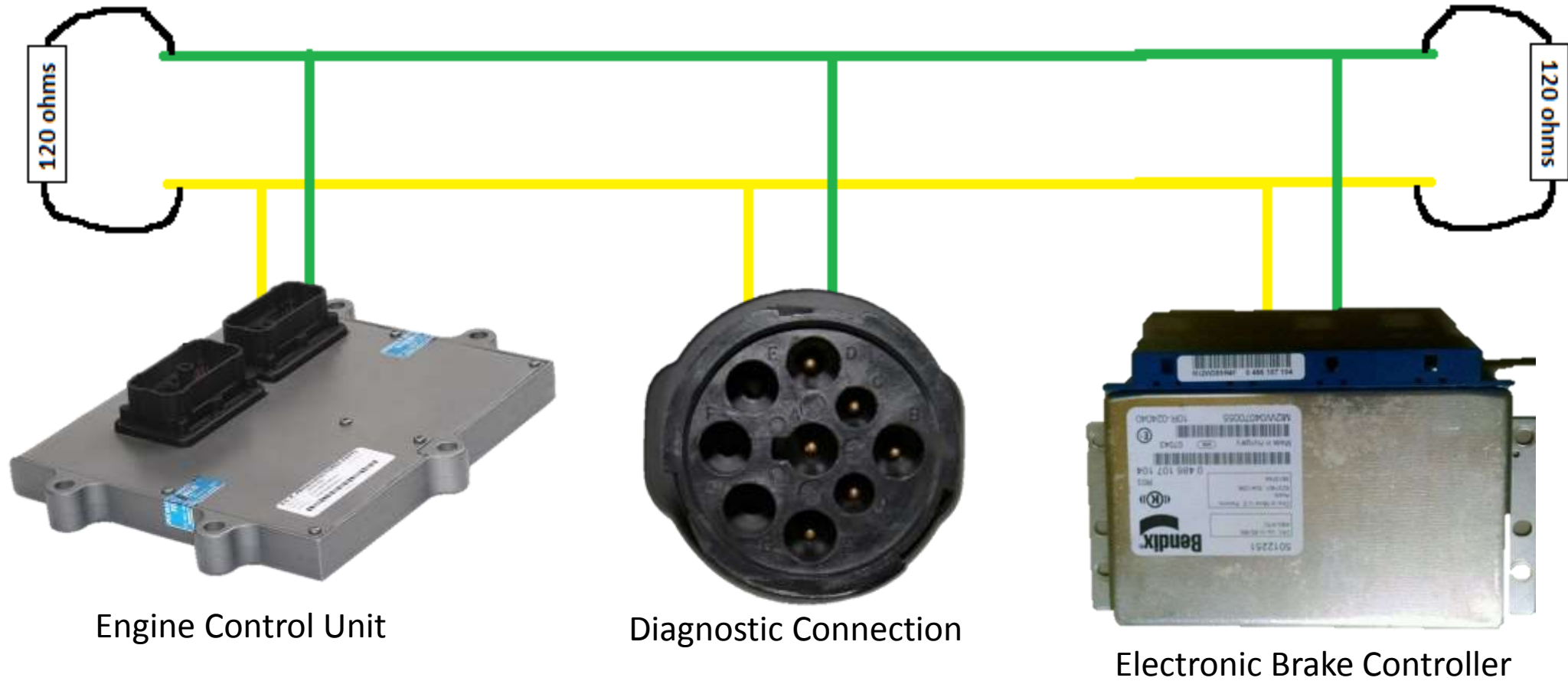
- In Heavy Trucks, CAN follows the J1939 Standard
 - Messages Have both ID and Data Field
 - Information is passed along the network from node to node



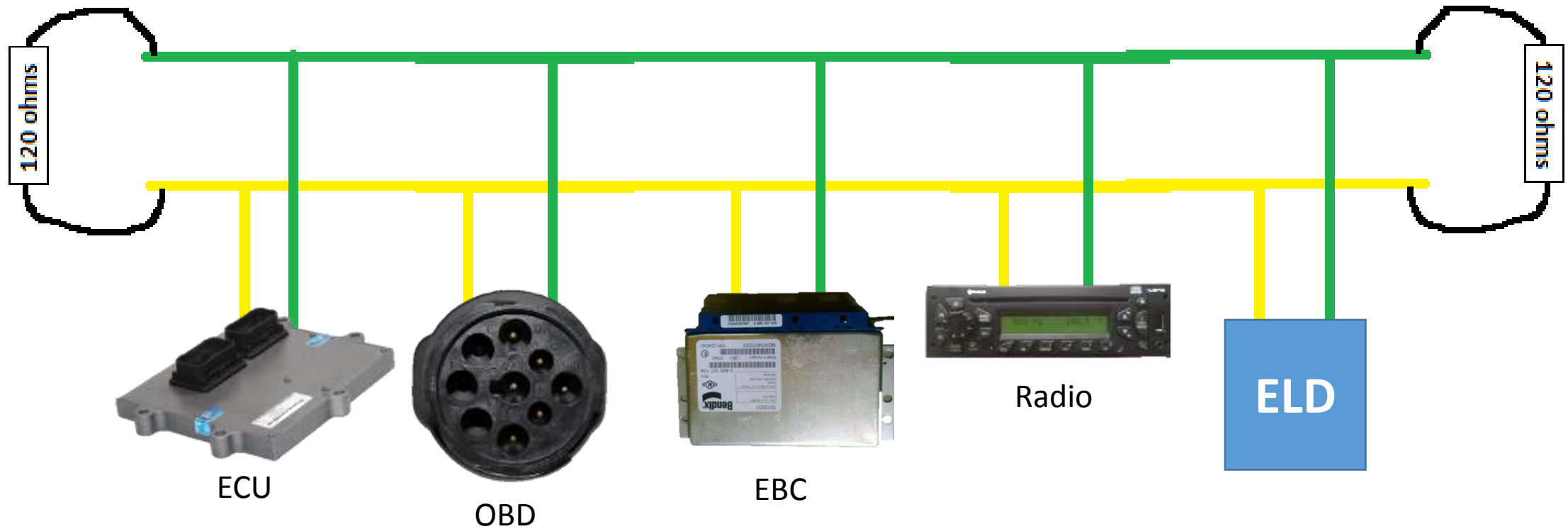
So what is connected?



THE UNIVERSITY of
TULSA
Student CyberTruck Experience



What else?



CAN Bus Downfall

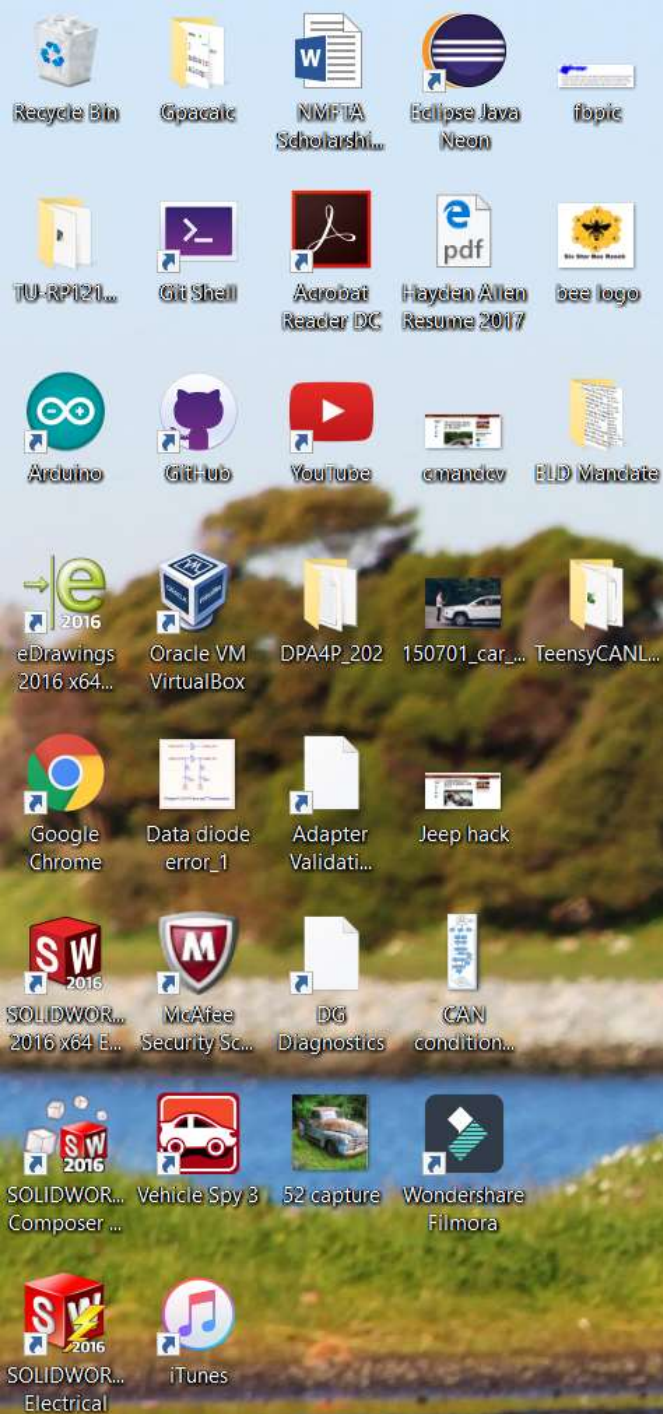
- No authentication
- No permissions
- If you can connect, you can read and send messages

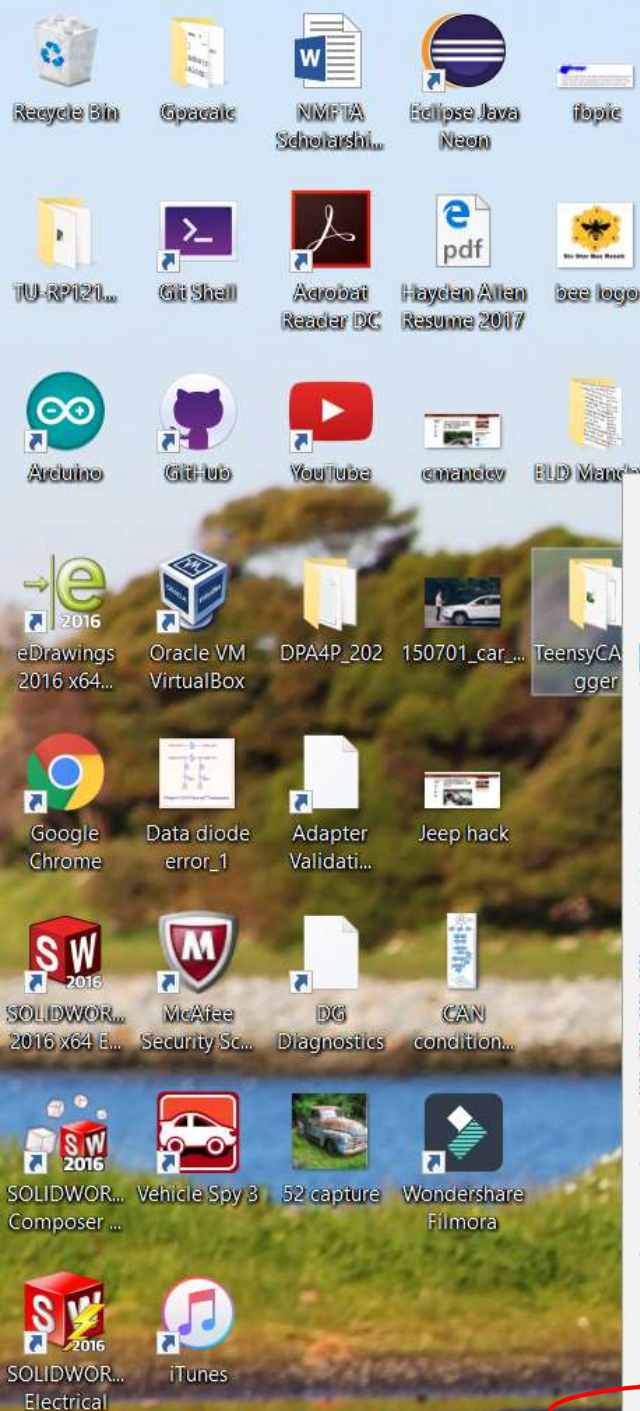


Wait, What Are Permissions?

- Tells the user what they are allowed to do within a file
 - Usually Read, Write, Execute
- What are some examples of these?







Open

- Pin to Quick access
- Add to VLC media player's Playlist
- Play with VLC media player
- Scan with Windows Defender...

Share with >

Restore previous versions

Include in library >

Scan

Shred

Pin to Start

Add to archive...

Add to "TeensyCANLogger.rar"

Compress and email...

Compress to "TeensyCANLogger.rar" and email

Send to >

Cut

Copy

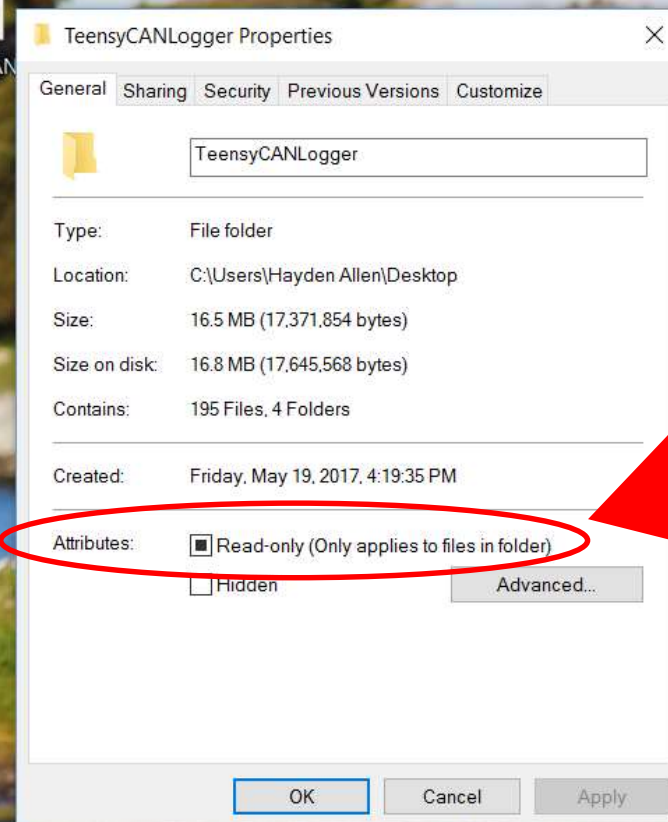
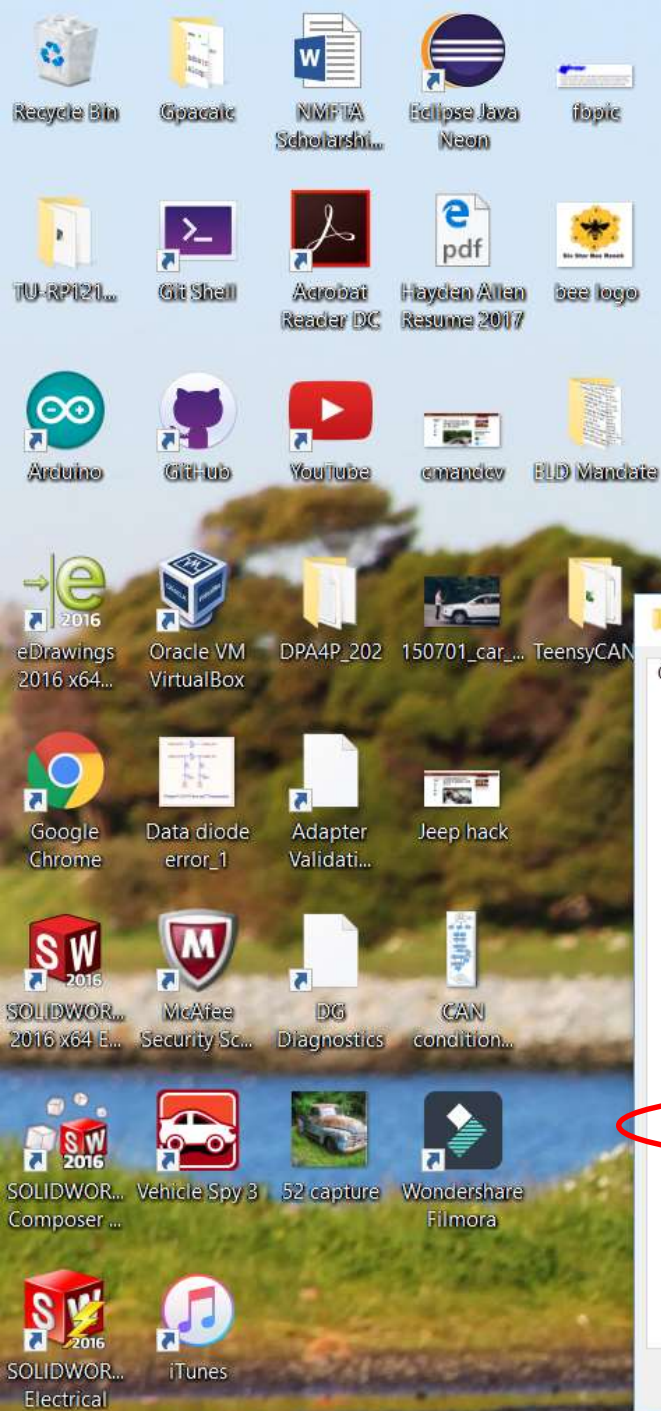
Create shortcut

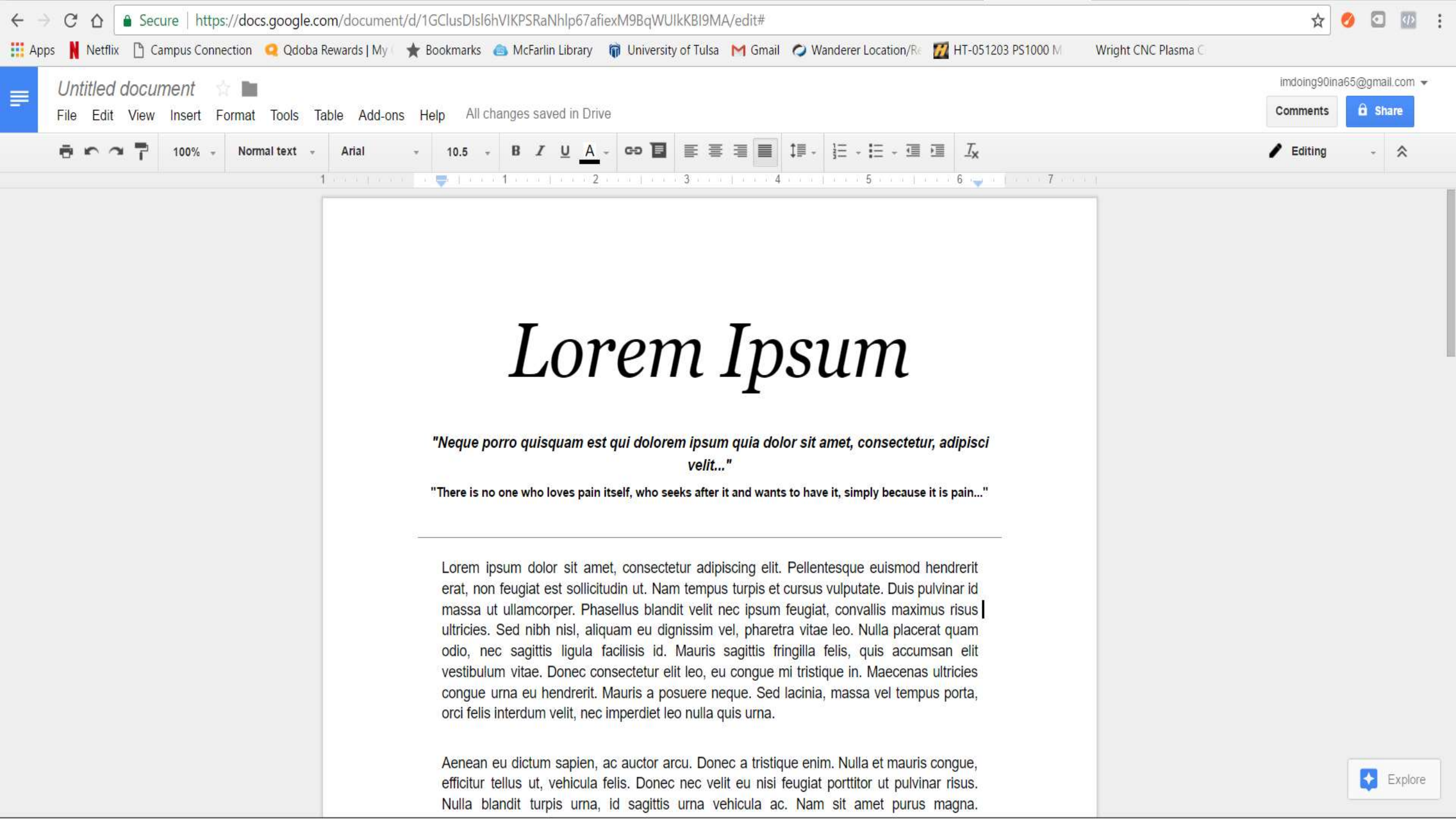
Delete

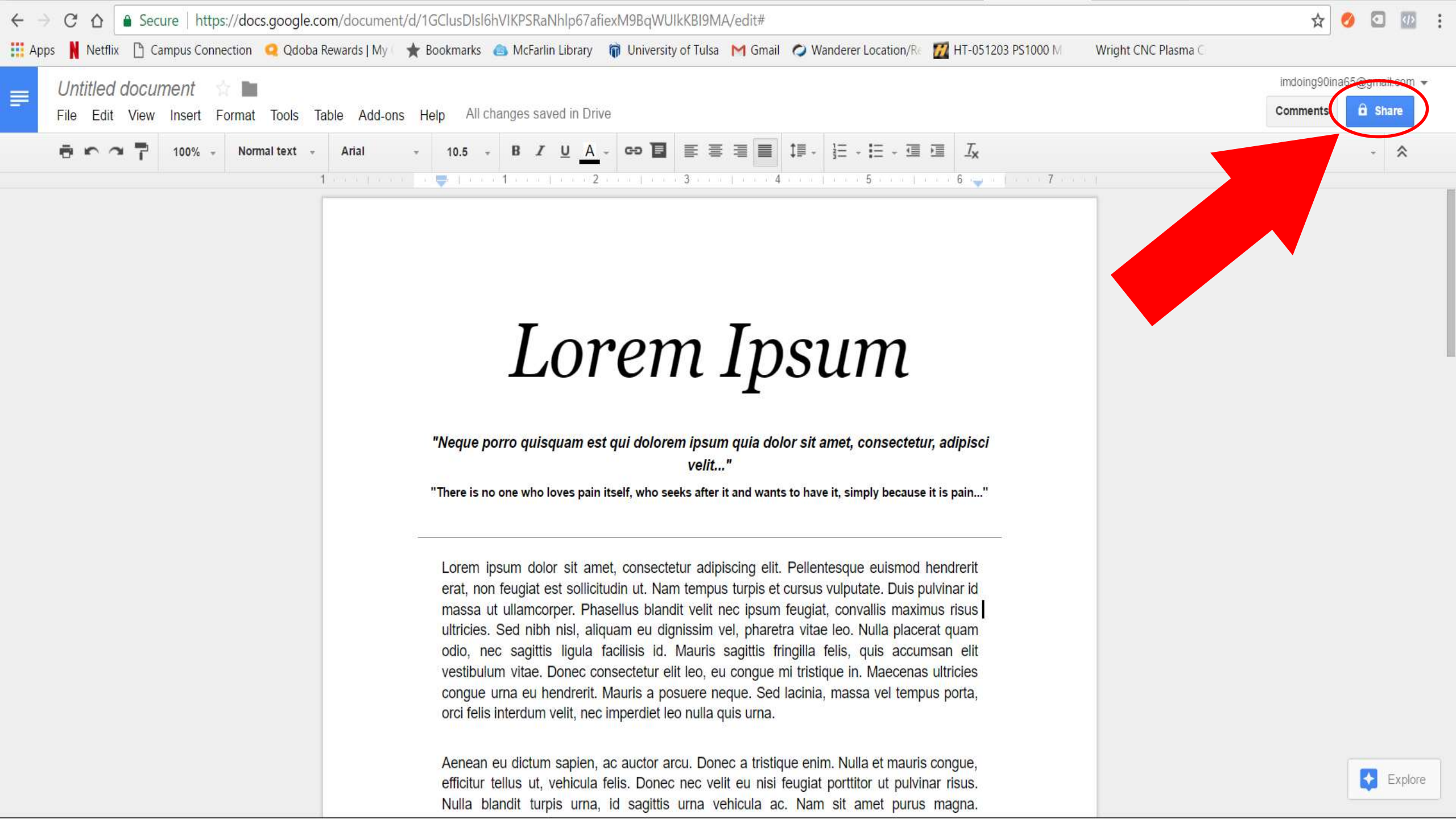
Rename

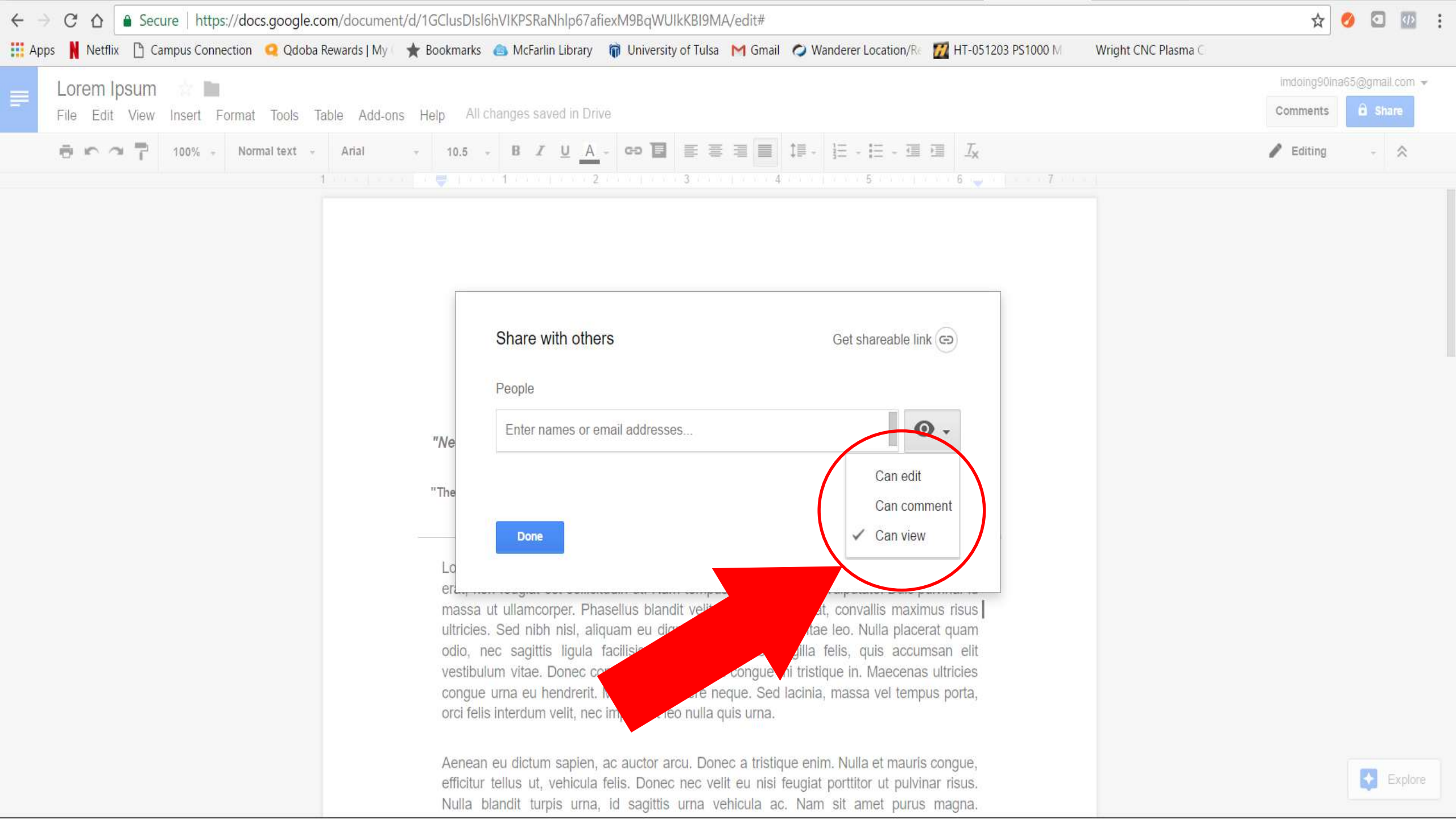
Properties





















What are permissions good for?


- Sharing Important Documents
- You do not want people to make changes to the documents you send them
- Dictates how the end user uses the shared file
- So what are the permissions in CAN?



					
Actual Bus	RW	RW	RW	RW	RW

					
Actual Bus	RW	RW	RW	RW	RW
Ideal Bus	?	?	?	?	?

					
Actual Bus	RW	RW	RW	RW	RW
Ideal Bus	RW	RW	RW	?	?

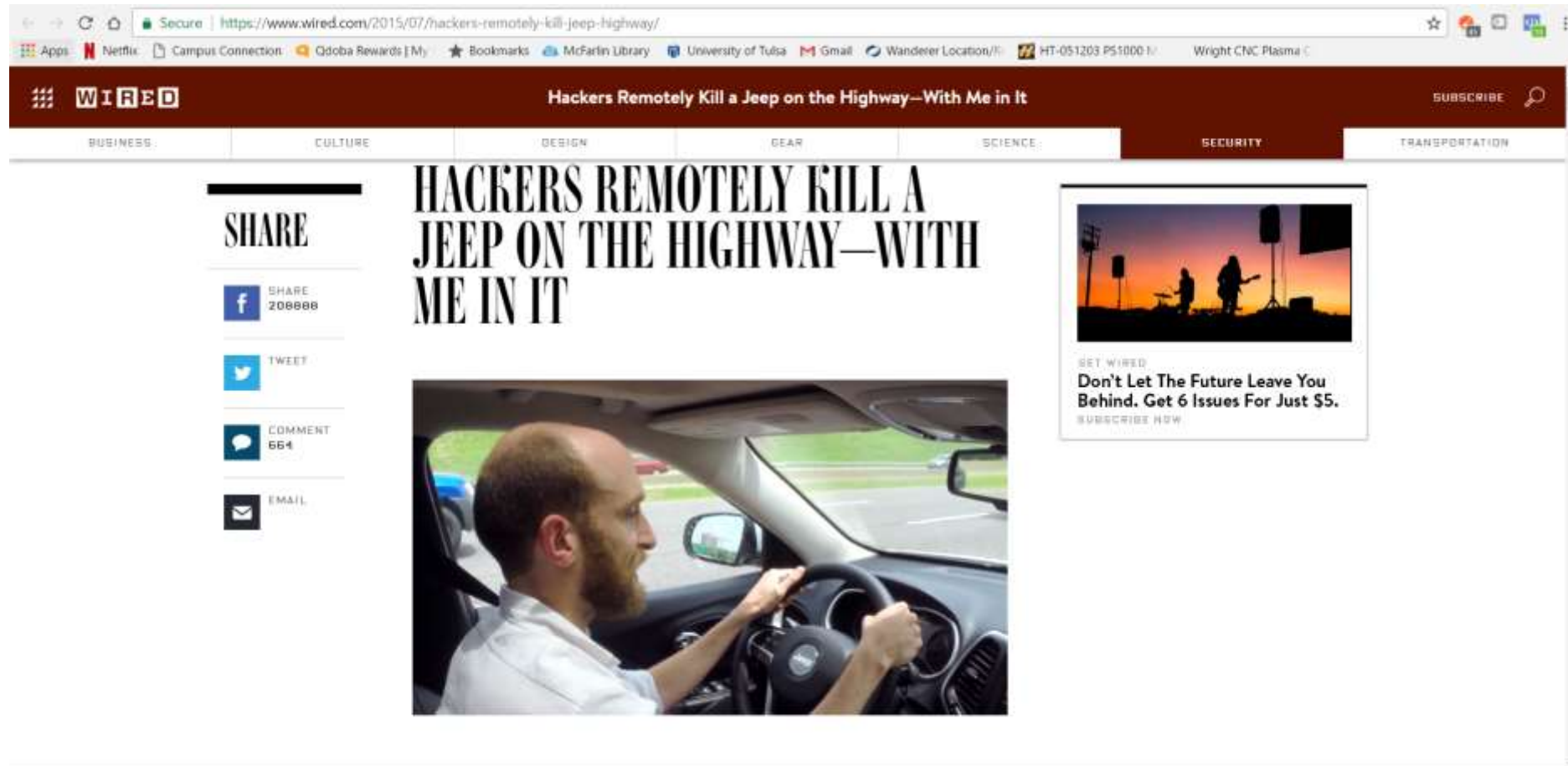
					
Actual Bus	RW	RW	RW	RW	RW
Ideal Bus	RW	RW	RW	?	?



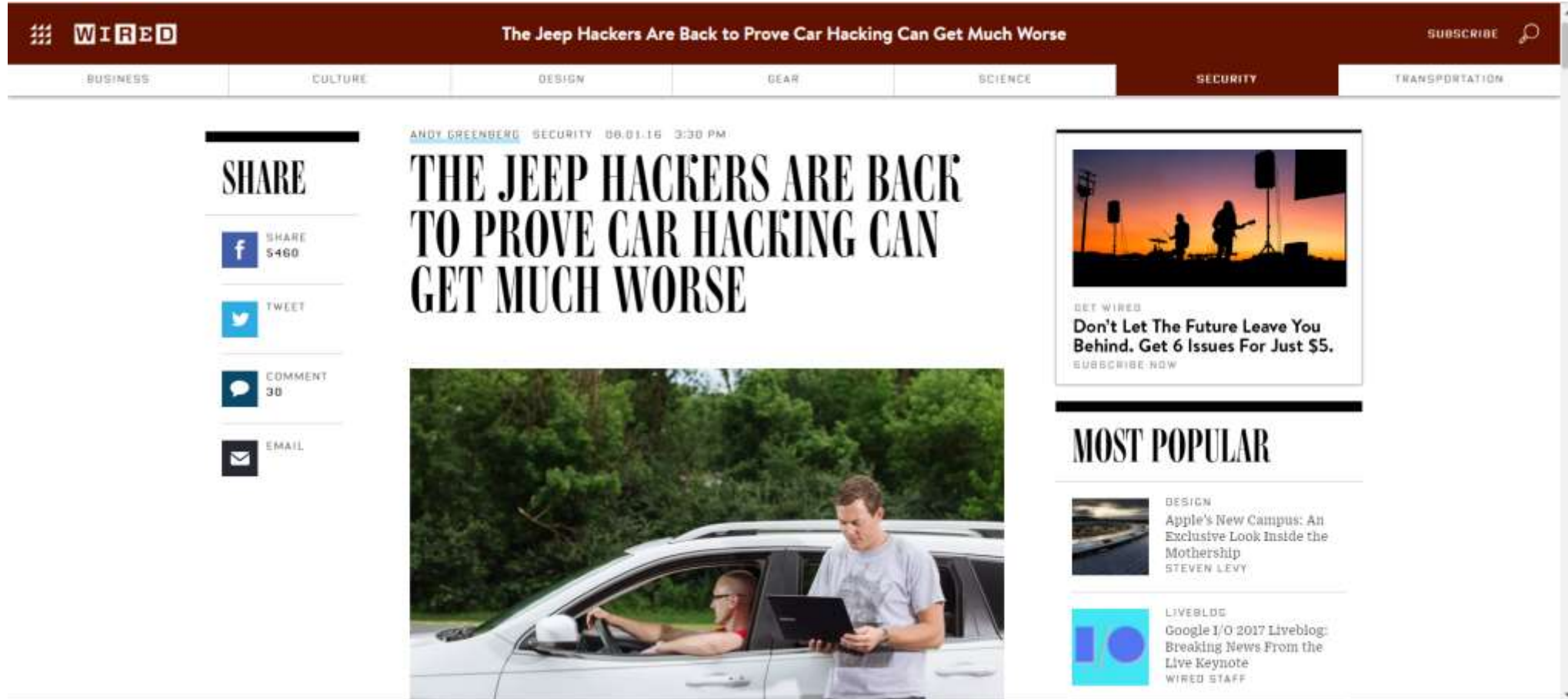
What could go wrong?



THE UNIVERSITY of
TULSA
Student CyberTruck Experience



What if you release a patch?



The screenshot shows the Wired website with a dark red header. The main article is titled "THE JEEP HACKERS ARE BACK TO PROVE CAR HACKING CAN GET MUCH WORSE" by Andy Greenberg, dated 08.01.16 at 3:30 PM. The article features a photo of a man in a grey t-shirt holding a laptop next to a silver car, with another person visible inside the car. To the left of the article is a "SHARE" section with icons for Facebook (5460 shares), Twitter, Comment (30), and Email. To the right is a "MOST POPULAR" section with two items: "Apple's New Campus: An Exclusive Look Inside the Mothership" by Steven Levy and "Google I/O 2017 Liveblog: Breaking News From the Live Keynote" by the Wired Staff.

WIRED

The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse

SUBSCRIBE

BUSINESS CULTURE DESIGN GEAR SCIENCE SECURITY TRANSPORTATION

SHARE

f SHARE 5460


TWEET

COMMENT 30

EMAIL

ANDY GREENBERG SECURITY 08.01.16 3:30 PM

THE JEEP HACKERS ARE BACK TO PROVE CAR HACKING CAN GET MUCH WORSE



GET WIRED
Don't Let The Future Leave You Behind. Get 6 Issues For Just \$5.
SUBSCRIBE NOW

MOST POPULAR

DESIGN
Apple's New Campus: An Exclusive Look Inside the Mothership
STEVEN LEVY

LIVEBLOG
Google I/O 2017 Liveblog: Breaking News From the Live Keynote
WIRED STAFF

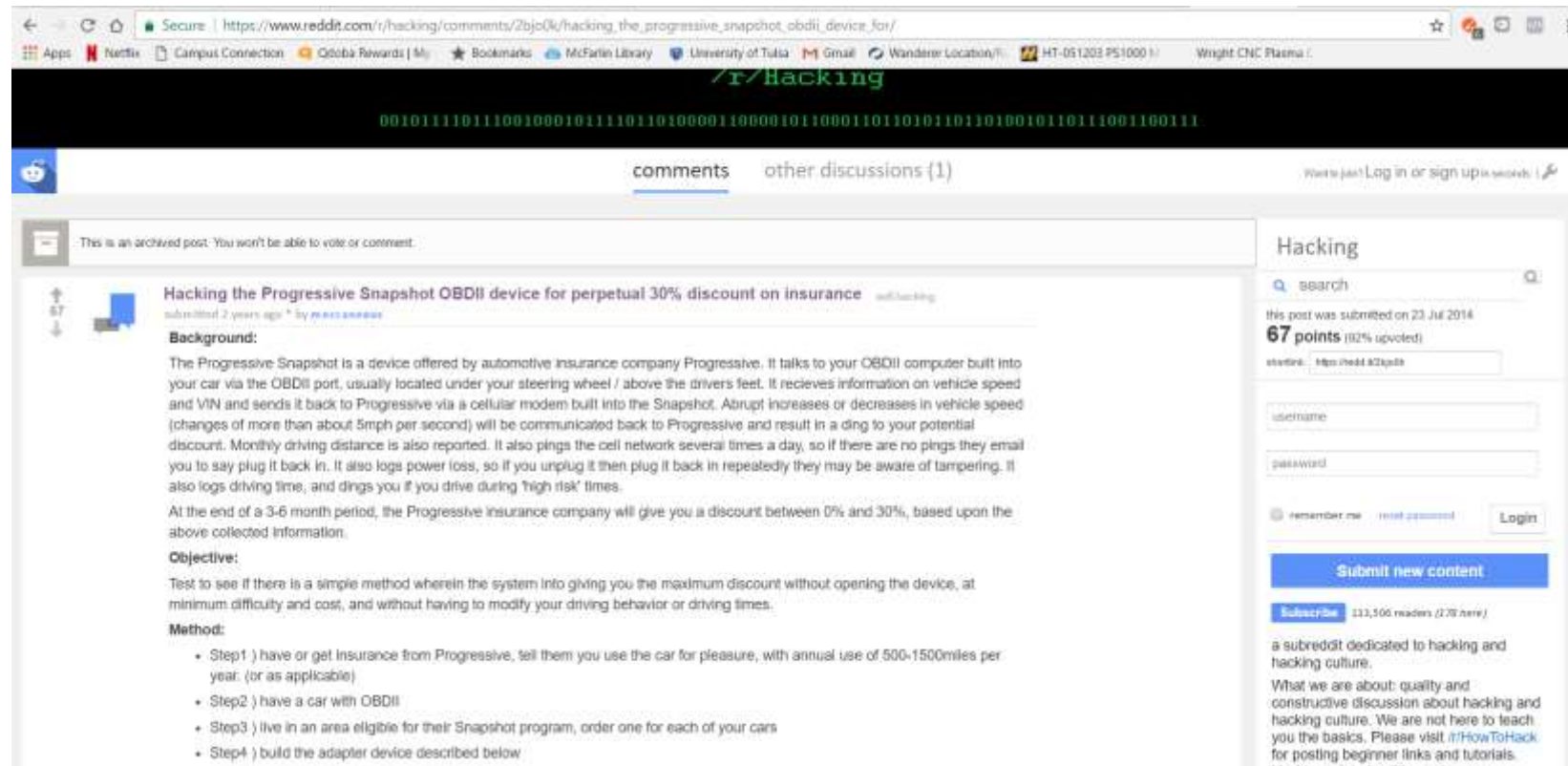
What Else Is Vulnerable?

- Electronic Logging Devices
 - Insurance Data Loggers







How?

- One simple web search tells you step by step what to do!



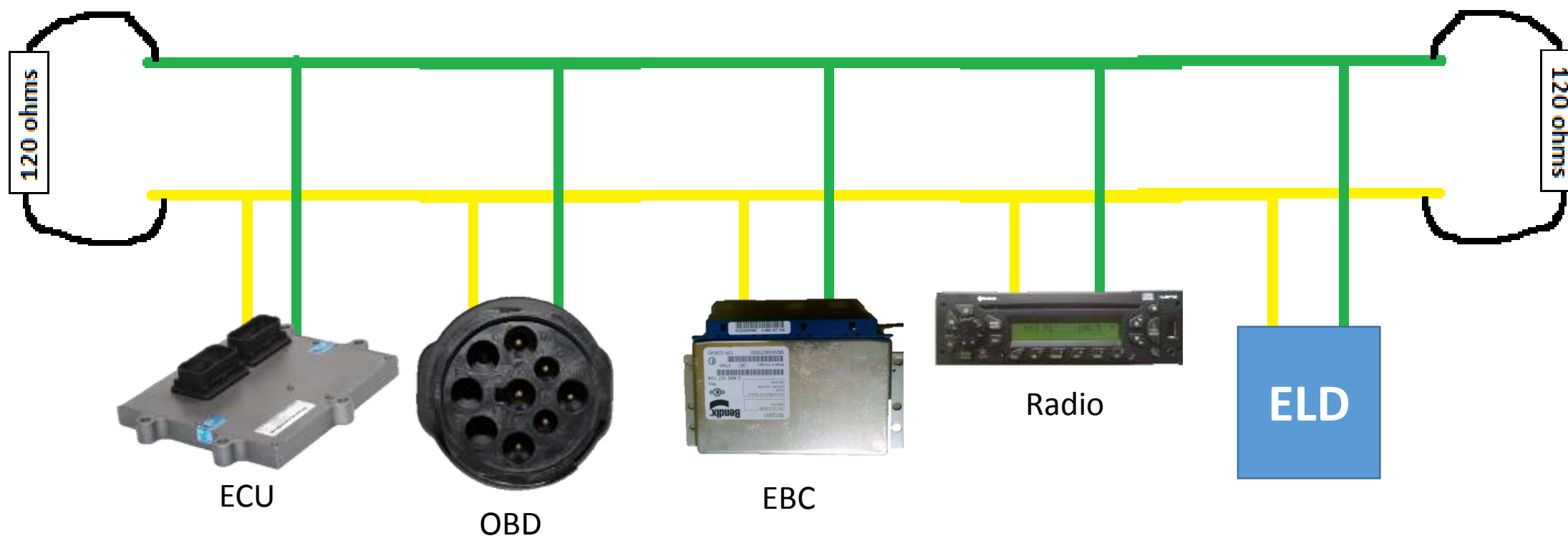


					
Actual Bus	RW	RW	RW	RW	RW
Ideal Bus	RW	RW	RW	R	R

CAN Bus



THE UNIVERSITY of
TULSA
Student CyberTruck Experience

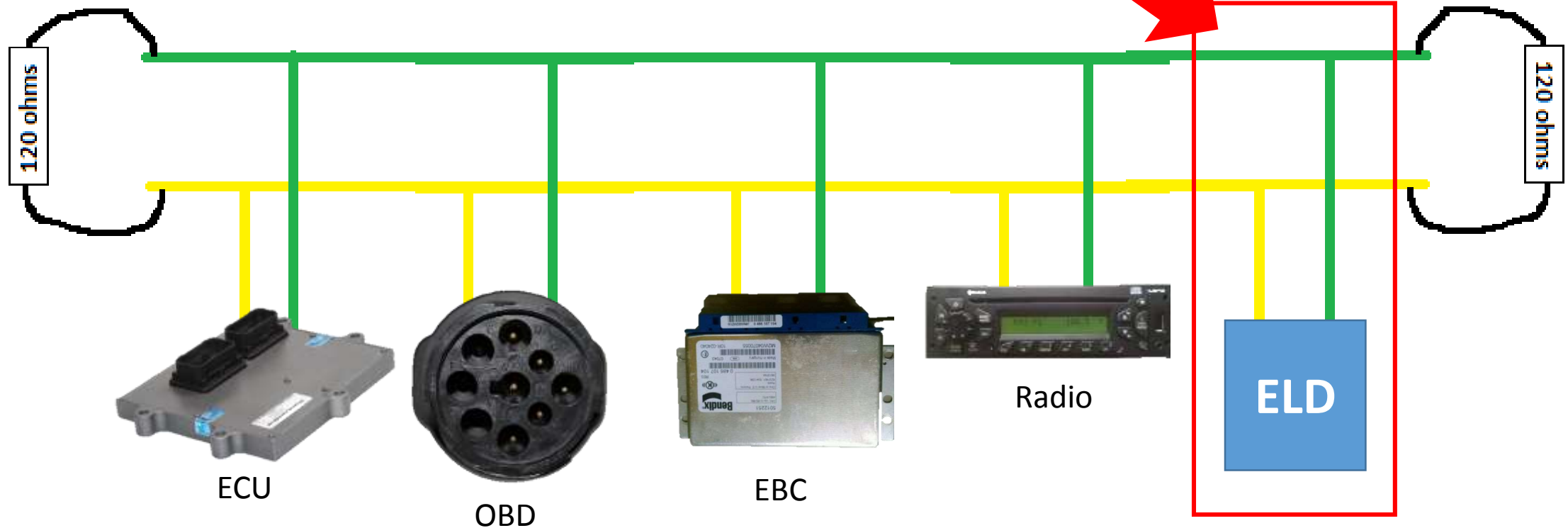


CAN Bus



THE UNIVERSITY of
TULSA
Student CyberTruck Experience

Let's look at
this section

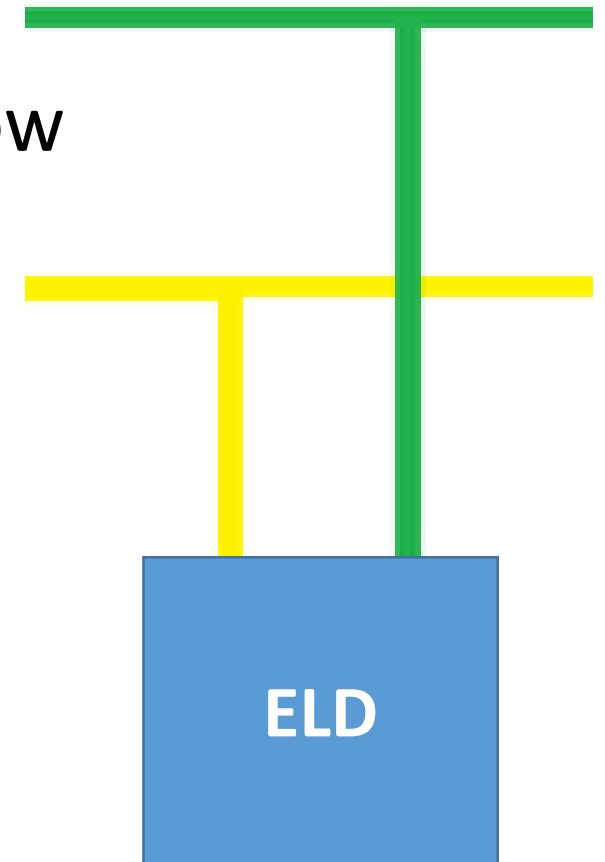


How Do You Achieve Read Only?



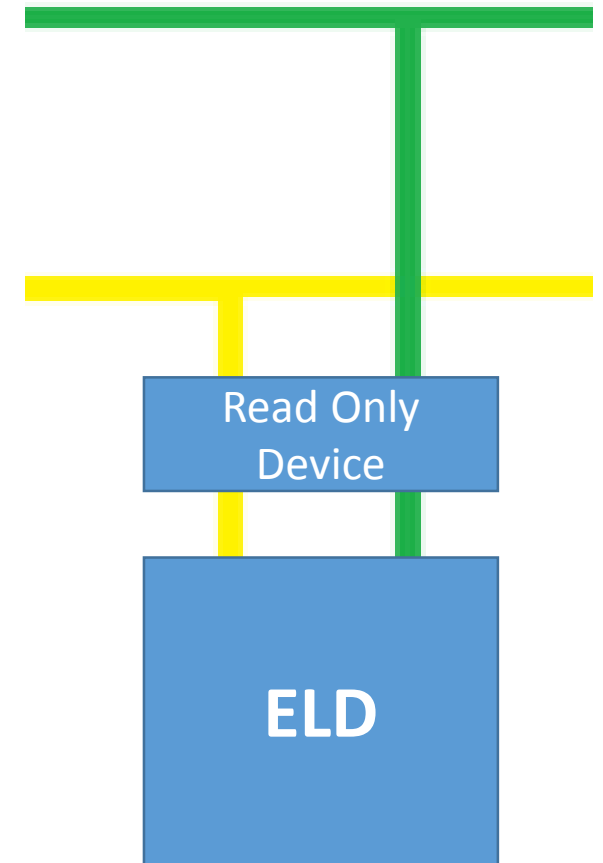
THE UNIVERSITY of
TULSA
Student CyberTruck Experience

- In order to achieve read only
 - Must allow messages in (READ) but not allow messages out (WRITE)
 - Must maintain functionality of the downstream device



Achieving Read Only

- Must have an additional device in place
 - Must be done through hardware
 - Software is vulnerable to attack and can be changed to allow for new functionality
 - Remember Miller and Valasek?
Progressive?



Data Diode

Establishing a more secure CAN bus

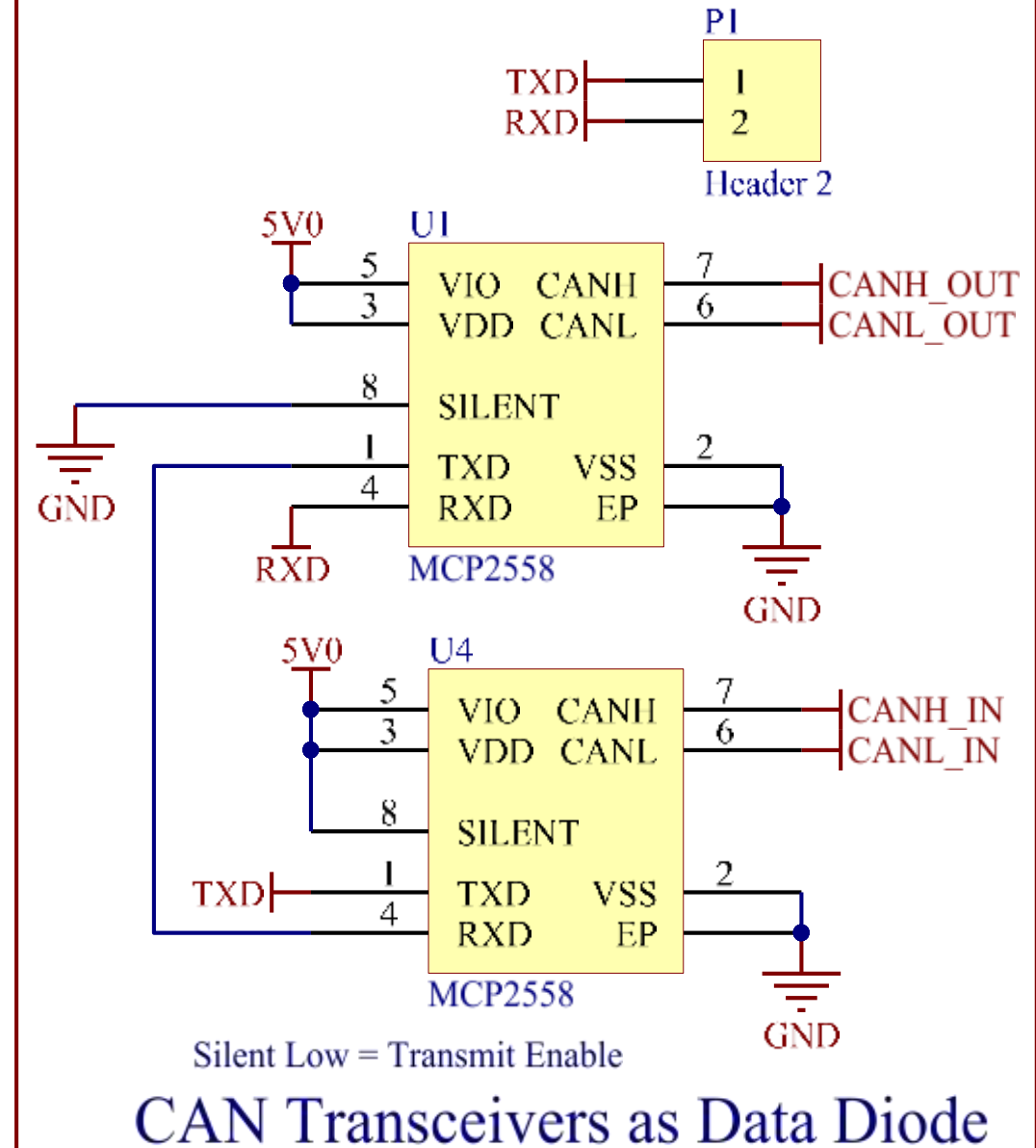
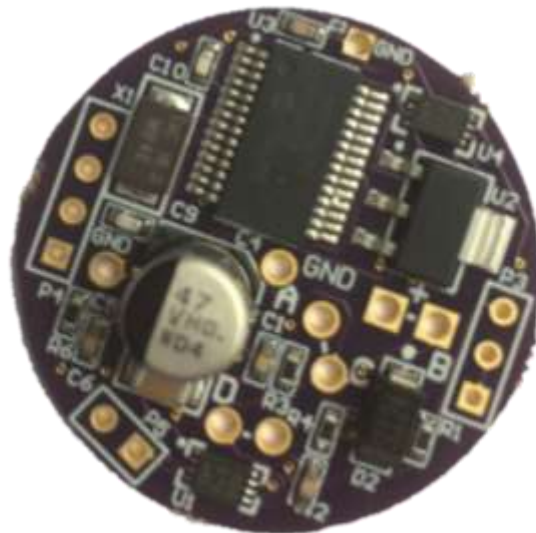


What is a Data Diode?

- Removes full bus write access
 - Accomplished by wiring TX and RX pins together on two separate CAN transceivers
 - This removes full write ability
- Maintains functionality of downstream devices
 - The data diode contains an extra controller and transceiver to acknowledge the downstream unit
 - This maintains full functionality of the downstream (ELD)



Schematics and Prototype



Assembly



Assembling the Backshell

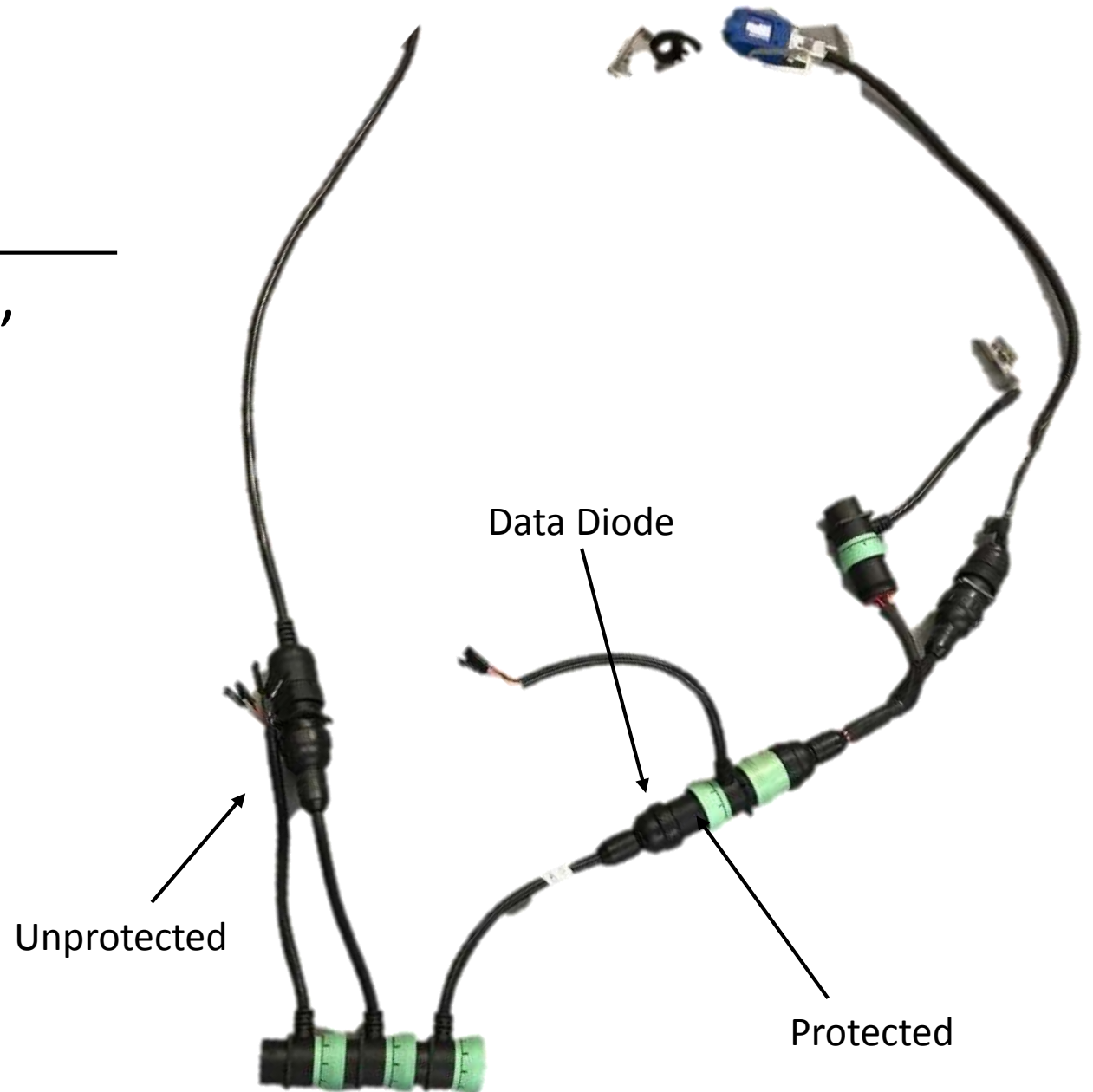


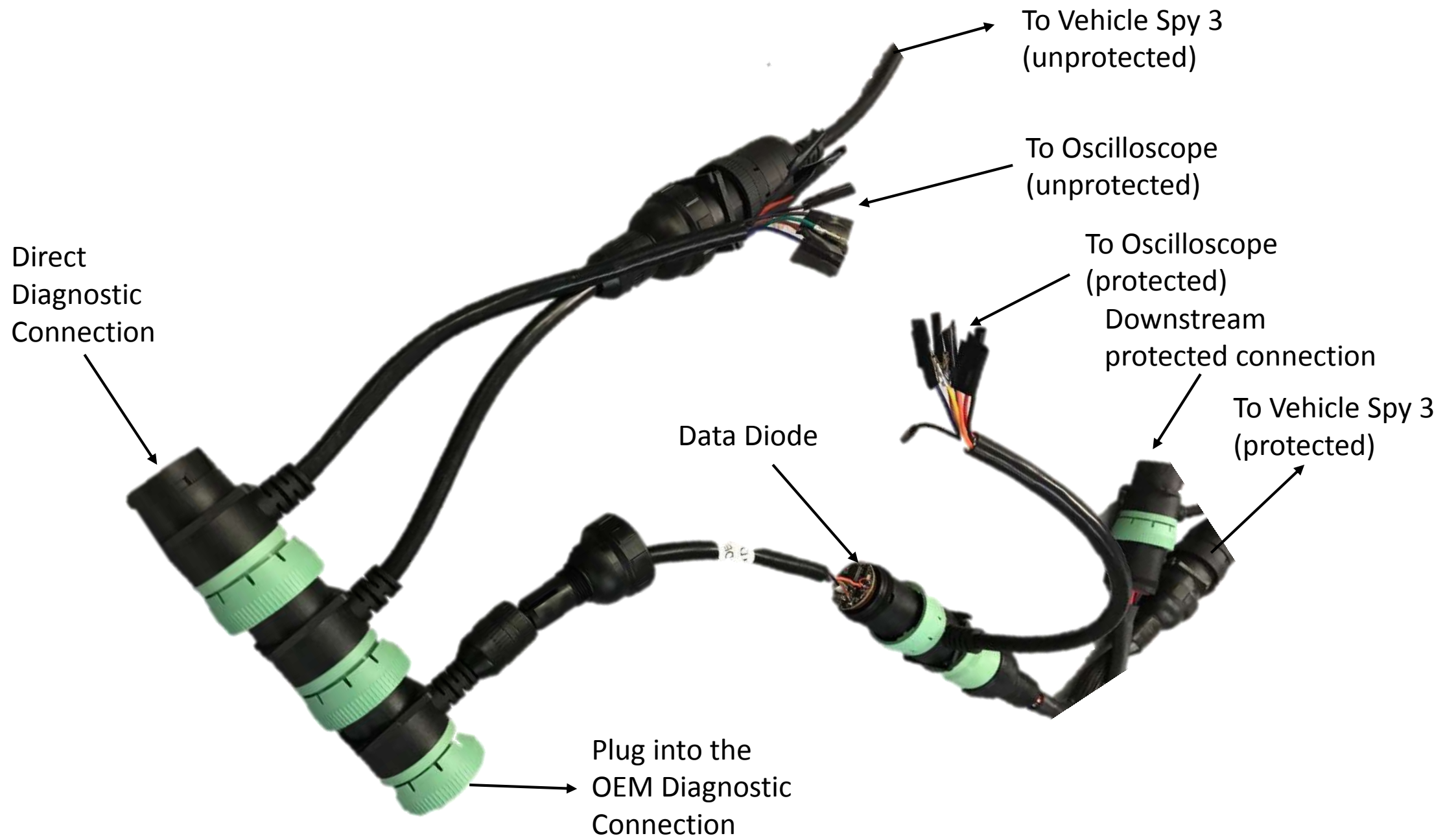


PROOF of Concept

Testing Setup

- In order to test the data diode, two branches were created.
 - Unprotected (J1939) – Directly connected to a truck or test bed through the Deutsch 9-pin
 - Protected (ELD) – Connected to diagnostic but is protected by the Data Diode







Adruino Teensy Tone Ring Frequency Generator

- Created to be able to display vehicle speed on a live bus
 - Offers a physical display of bus functionality
- A Teensy 3.2 Arduino that is emitting a frequency into the tone ring input on the test Cummins ECM
- A potentiometer is used to change the output frequency



RIGOL

T'D

H

5.000ms

100.0MSa/s
7.00M pts

D

278.800000us

T

f

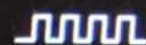
310mV

HORIZONTAL

J1939 Bus

ELD Bus

AUTO



Undo

1 = 100mV

2 = 100mV

11:17

Denial-of-Service

- DOS attack
 - Works by sending the inherent highest priority message
 - ID = 0x00;
 - Simple attack to execute
 - When implemented, all bus communication ceases
 - Visually evident by gauge cluster no longer displaying the speed from the tone ring frequency generator

```
1 #include <FlexCAN.h>
2 #include <kinetis_flexcan.h>
3
4 FlexCAN J1939bus(250000);
5 static CAN_message_t txmsg, rxmsg;
6
7 void setup() {
8     J1939bus.begin();
9     txmsg.id = 0x00000000;
10    txmsg.len = 8;
11    txmsg.ext = 1;
12    txmsg.buf[0] = 0x00;
13    txmsg.buf[1] = 0x00;
14    txmsg.buf[2] = 0x00;
15    txmsg.buf[3] = 0x00;
16    txmsg.buf[4] = 0x00;
17    txmsg.buf[5] = 0x00;
18    txmsg.buf[6] = 0x00;
19    txmsg.buf[7] = 0x00;
20 }
21 void loop() {
22     J1939bus.write(txmsg);
23 }
```


RIGOL

TD

H

5.000ms

100.0MSa/s
7.00Mpts

D

278.800000us

T

310mV

HORIZONTAL

AUTO

J1939 Bus

Diode Bus

1 = 100mV

2 = 100mV

Undo

11:18



RIGOL

TD

H

5.000ms

100.0MSa/s
7.00M pts

D

278.800000us

T

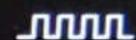
f

310mV

HORIZONTAL

J1939 Bus

AUTO



Undo

Diode Bus

1

= 100mV

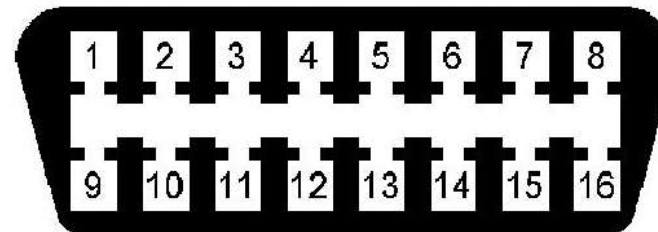
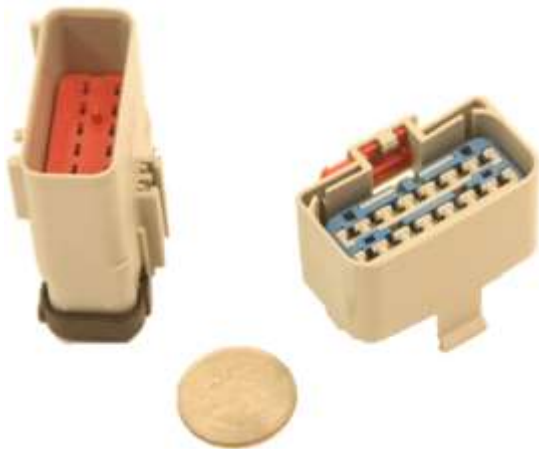
2

= 100mV

11:18

Potential Implementations

- Direct In-Line Connection
 - As displayed in testing
- Dsub 15 Connection
- Delphi 14 pin Connection
- J1962 OBD-II Connection



Data Diodes w/ Requests



Some Requests Handled by Other Nodes



- However, with the Data Diode, an ELD will be unable to request any additional information
 - For Example:
 - VIN Number
 - Engine Hours
- The ELD is not the only node that may need to know this information
 - For example, an instrument cluster may request Engine Hours from the ECM

Requesting Enabled Diodes

- A potential solution:
 - Implementing a requestor that sends out timely request messages
 - Operates parallel to the ELD
 - Connected to J1939 network
 - Not directly connected to the ELD network
 - Would send out request messages so that the responses are logged by the ELD
- Design is done, but boards have to be built.





Why Is This Important?

2015 ELD Mandate

- Mandates that all trucks 2000 or newer will be required to have an Electronic Logging Device installed on all trucks.
- Why?
 - Taken from the first sentence within the mandate:
“This rule improves commercial motor vehicle (CMV) safety and reduces the overall paperwork burden for both motor carriers and drivers by increasing the use of ELDs within the motor carrier industry” – FMSCA 2015



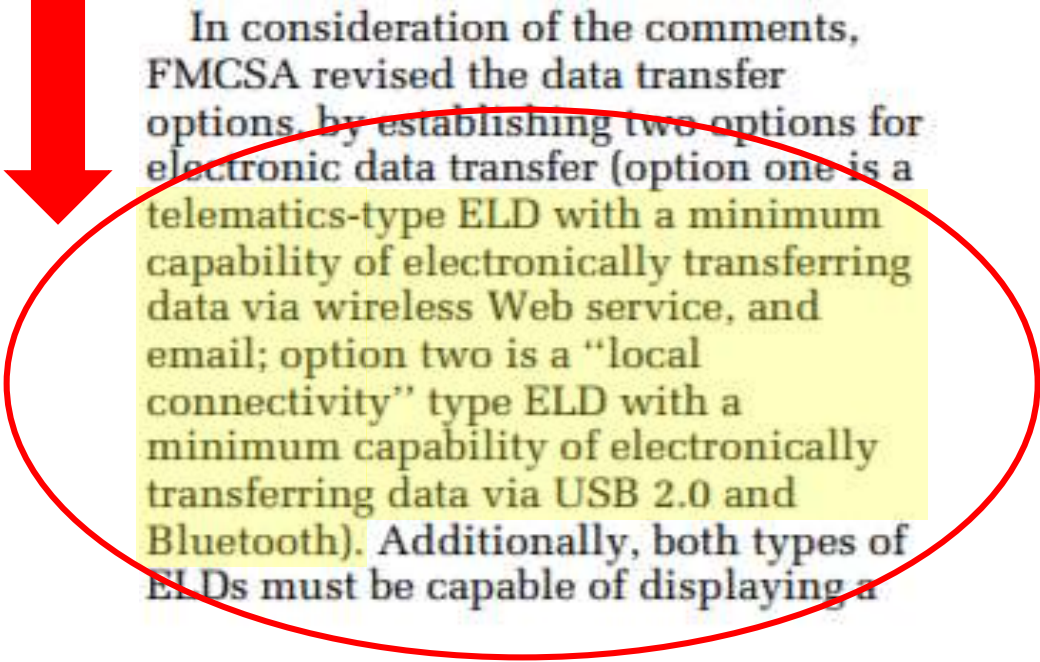
Downfalls of the Mandate

- Mandate adds additional attack vectors to Heavy Vehicles
 - Attack Vector: A path or means by which a hacker (or cracker) can gain access to a network.



How are they doing this?

- Adding Internet Connectivity
- Adding Bluetooth and USB 2.0



In consideration of the comments, FMCSA revised the data transfer options by establishing two options for electronic data transfer (option one is a telematics-type ELD with a minimum capability of electronically transferring data via wireless Web service, and email; option two is a “local connectivity” type ELD with a minimum capability of electronically transferring data via USB 2.0 and Bluetooth). Additionally, both types of ELDs must be capable of displaying a

1. Comments to the 2014 SNPRM

Proposed section 4.10.1 provided that ELDs must transmit records electronically in accordance with a specified file format and must be capable of a one-way transfer of these records to authorized safety officials upon request. Proposed section 4.10.1.1 described the standards for transferring ELD data to FMCSA via Web services.

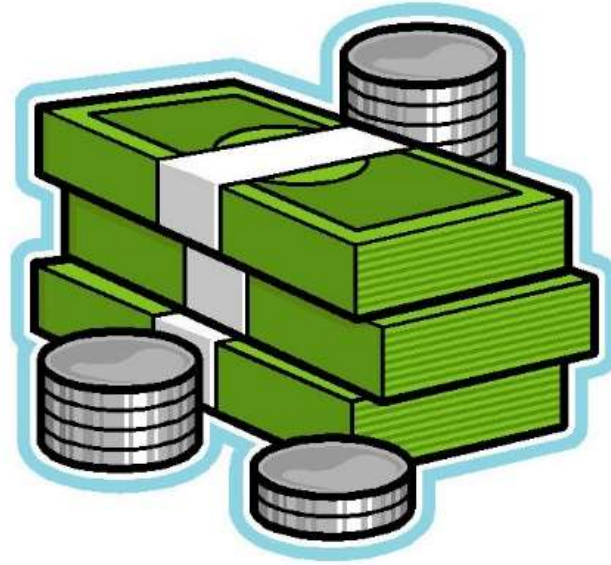
BigRoad stated that section 4.10.1.1 describes how an ELD provider must obtain a public/private key pair compliant with NIST SP 800 32. Using a private key in this scenario is not ideal since it would have to be stored on every ELD that might create the email and is therefore exploitable via memory inspection or code disassembly.

2. FMCSA Response

All required security measures for data transfer with the Agency, public or private, will require strict adherence to NIST for all data in transit or ‘handshakes’ between Government and private systems. DOT guidelines follow NIST 820. The exact Public Key Infrastructure (PKI) for ELD data transfers will be distributed once ELD providers register and certify ELDs.



THE UNIVERSITY *of*
TULSA
Student CyberTruck Experience



How Much Does It Cost?

Adding an ELD

- The FMSCA projects that adding a web supported ELD will cost \$419 annually, with an initial purchase price of \$500/unit.
- USB 2.0 or Bluetooth ELDs will cost \$166 annually.
- How much would adding a diode cost?

In today's rule FMCSA estimates the annualized cost for an ELD that must support one of two options for electronic transfer. The first option is a telematics type ELD. We estimate a total annualized cost of \$419 for an ELD with telematics. The RIA prepared for the SNPRM assumed an annualized device cost of \$495, which FMCSA acknowledged was on the high end of the range of costs of existing units. The \$495 figure cited by OOIDA is therefore no longer relied upon by the Agency. The reduction in the estimated annualized cost for an ELD with telematics, from \$495 to \$419, is largely attributable to the reduction in purchase price of the device from \$799 to \$500. The second option is a local transfer method type ELD (ELD with USB 2.0 and Bluetooth). The estimated annualized cost of an ELD with USB 2.0 and Bluetooth is \$166. The lower price



Quote 68022

Reference Quote Number

68022

Data Diode Prototyping Costs

- Amphenol/Deutsch 9-pin Connector: \$9.22
- 4 Deutsch PCB pins: \$8.00
- M/F J1939 Type II Pigtail Cable: \$11.84
- CAN Data Diode Assembled Printed Circuit Board: \$72.49
- Backshell and Compression Nut: \$7.05
- 0.25 Hours Assembly: \$5.00
- Total: \$113.60

Customer Name:	Buyer/Contact	Contact Information:	Part# - Rev	PCB Rev:
University of Tulsa	Jeremy Daily	jeremy-daily@utulsa.edu	CanDiodeWTXRX	

Base Quote (Quantities & Days)		Quote Specifications (Counts Per Board)	
Select One Base Quote			
<input checked="" type="radio"/> 25 Assemblies, 5 Day; Parts; PCBs 5 Day	\$1,489.53	SMT / THT Count:	18 / 0
		Line / Fine Pitch Count:	11 / 0
		X-Ray Count:	0
		Assembly Sides:	Top
		Assembly Types:	SMT&THT
		RoHS Required:	YES
		ITAR Required:	NO
Options			

Quoted By:	Date:	Email:	Phone:
Ashlie Johns	4/19/2017	ajohns@aapcb.com	720-484-3013

☐ Add Shipping Acct: Example: "UPS 12F3Y4"

AA Overnight

Discount: \$-250.00
 Order Total: \$ 1,762.30
 Per Board: \$ 70.49
 11 Business Days

Total Includes Shipping and NRE

[Place Order](#)

Understanding the Current Design



- Cost would drop if production scales.
- Over the Air Updates are incompatible
 - No write access prevents the telematics device from being able to write to the bus.
- If data needs requested (i.e. VIN), a separate node must do the job.
- Patent Pending
 - University of Tulsa filed for a utility patent

Acknowledgements



This material is based upon work supported by National Motor Freight Traffic Association, Inc (NMFTA), PeopleNet, and Geotab. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect those of NMFTA, PeopleNet, and Geotab.

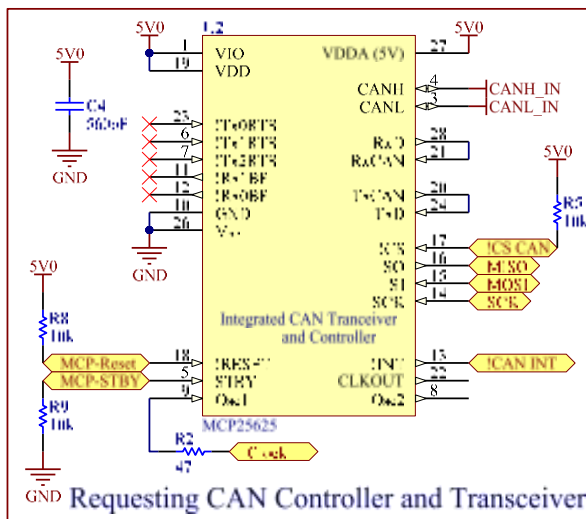
Questions?

Name: Hayden Allen

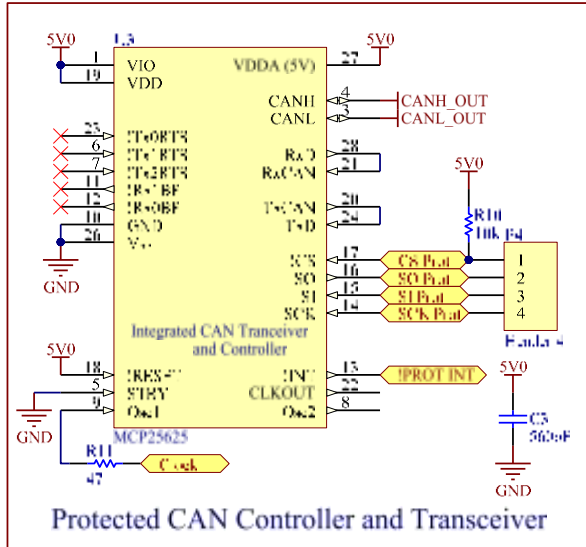
Email: hayden-allen@utulsa.edu

Phone: (918) 645-4938

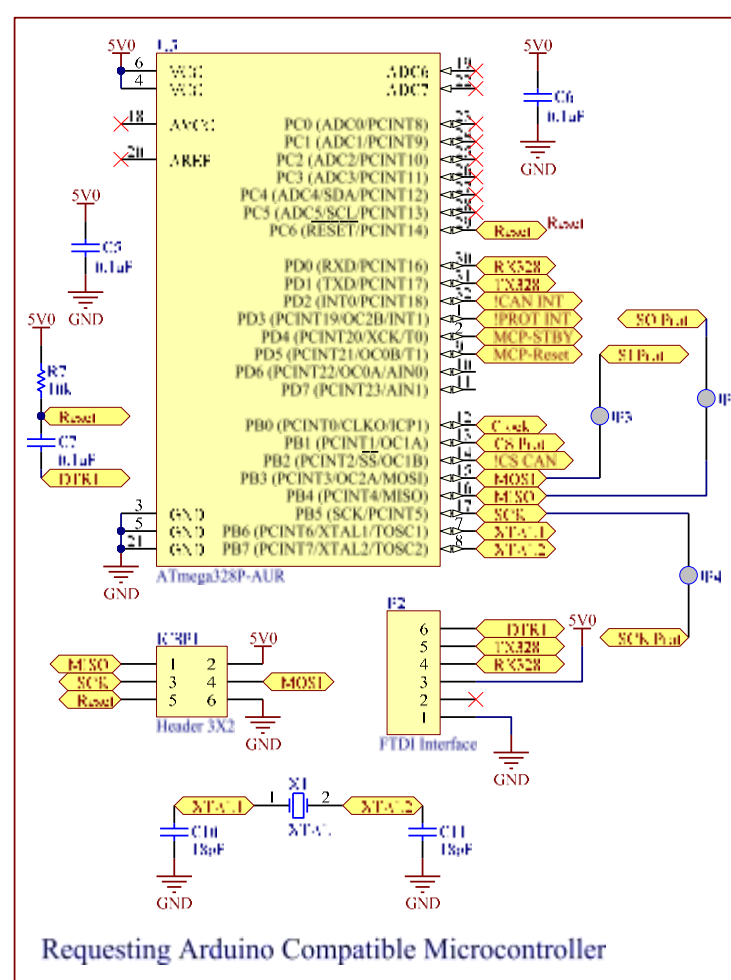




Requesting CAN Controller and Transceiver



Protected CAN Controller and Transceiver



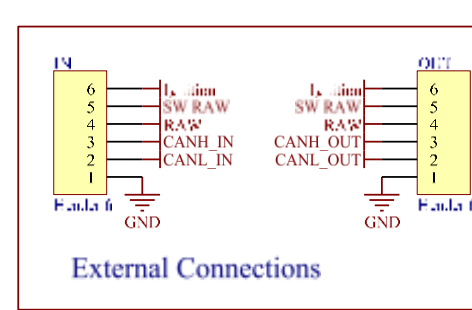
Requesting Arduino Compatible Microcontroller

Pinouts according to TMC's RP1226 for 14 Way Apex 2.8

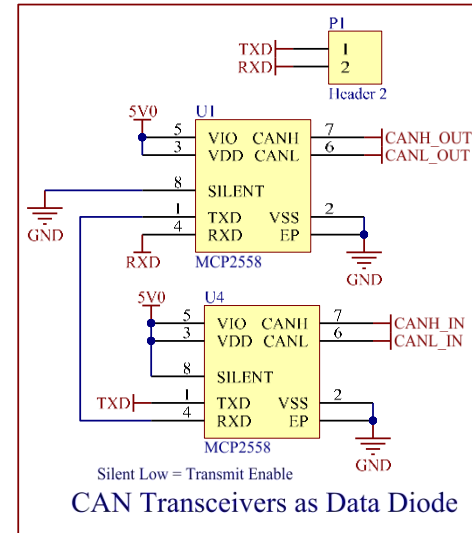
Apex	Signal	Color	Port Pin
1	SW_BATT	PNK	5
2	CAN_1_H	YEL	3
7	IGN	ORN	6
8	GND	BLK	1
9	CAN_1_L	GRN	2
14	BATT	RED	4

Use Delphi Part Number 54101416
(14 way male connector) for the CAN_IN
Male Unsealed terminals are Delphi/FCI Part 10762775

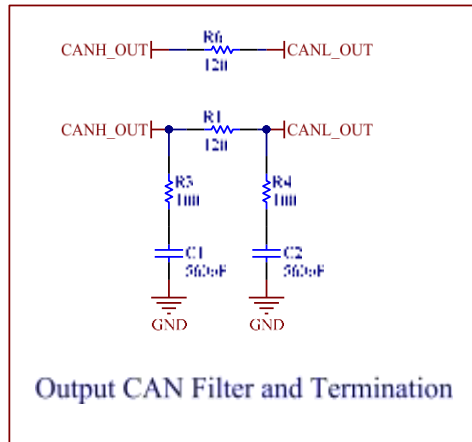
Use Delphi Part Number 54101412
(14 way female connector) for the CAN_OUT
Female Unsealed Terminals are Delphi/FCI Part 10757690



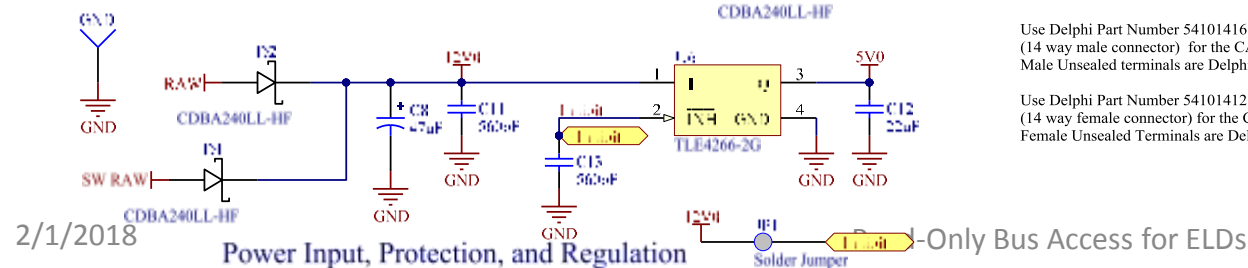
External Connections



CAN Transceivers as Data Diode



Output CAN Filter and Termination



Power Input, Protection, and Regulation

Only Bus Access for ELDs