

Heavy Vehicle Networks and Chip Level Forensics

Jeremy Daily, Ph.D., P.E.

Jeremy.Daily@colostate.edu



SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Heavy Vehicle Networks

Understanding SAE J1939 and CAN data



SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Chip Level Forensics

Extracting and decoding data from memory in electronic control units



SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Scope

- Chip level forensics is the process of extracting and decoding data from memory bearing chips inside electronic control units
- Utilized when network based forensics (i.e. downloads and diagnostics) are not tenable
- Board level and chip level forensics are treated similarly



Network Level

Data collected using a vehicle network or bench setup

- Cummins PowerSpec
- Bosch CDR Tool

Board Level

Data collected through internal debug and programming ports

- KTAG
- PE Micro

Chip Level

Data collected from a chip extracted from the board and read using a chip reader

- Xeltek Super Pro

Hybrid: Chip Transplants



Problem Statement

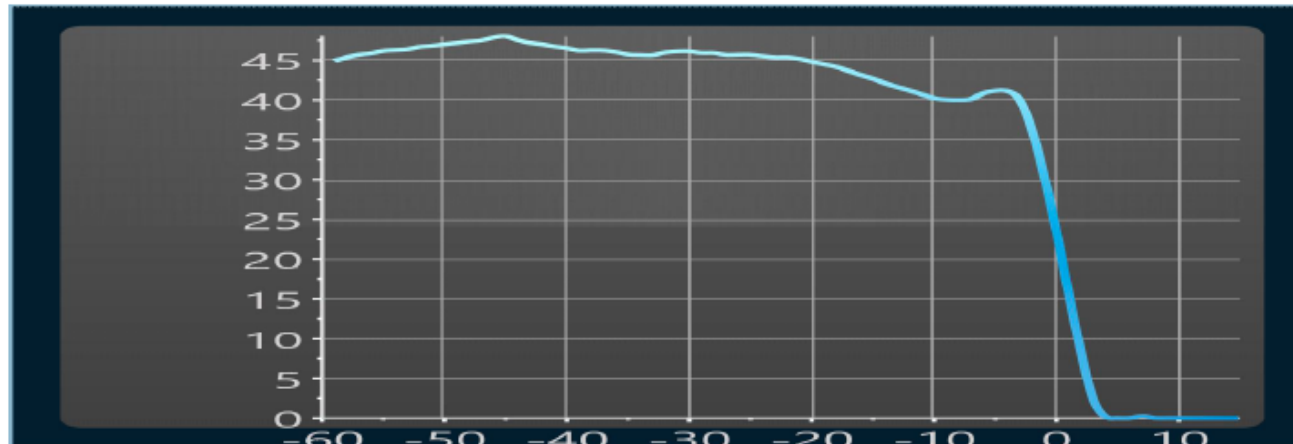
- We want to connect to a truck...



Vehicle Sudden Deceleration Report Record 1

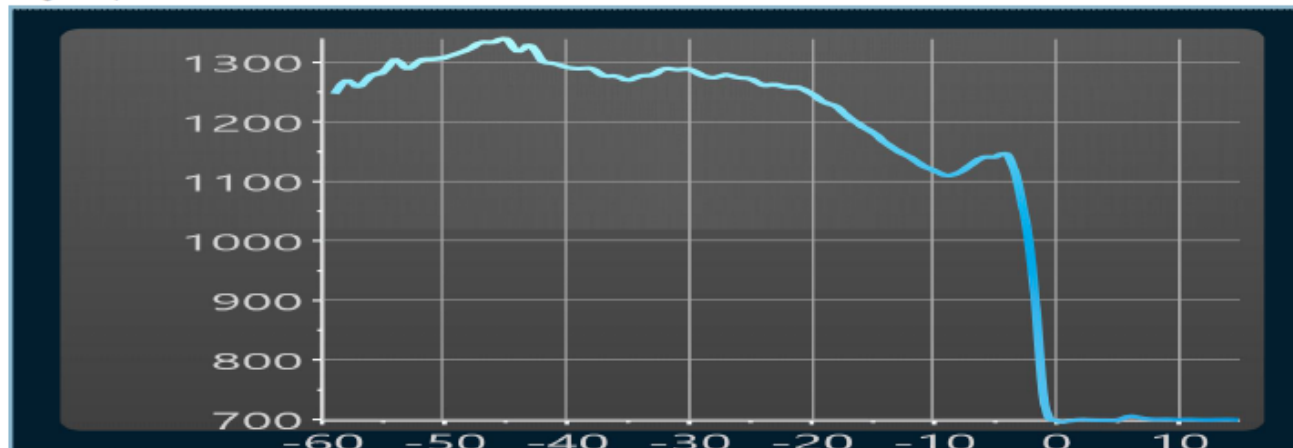
Engine Type	ISX 2013	Ecm Code	EF10067.34
Engine Serial Number	79749226	Software Phase	9.40.0.53
Unit Number	0000000000	Extraction Date	09-18-2017 10:00:16
Sudden Decel Threshold Rate:	7.00 mph	ECM Run time	8120:27:45
Occurrence Date: N/A		ECM Run Time at Occurrence: 7472:53:17	
Air Temperature (°F) at Occurrence: 69		Occurrence Distance (mi): 371978.5	

Vehicle Speed



...and get data.

Engine Speed



Example from
Cummins PowerSpec

Engine Control Module Location



Engine Control Module Location

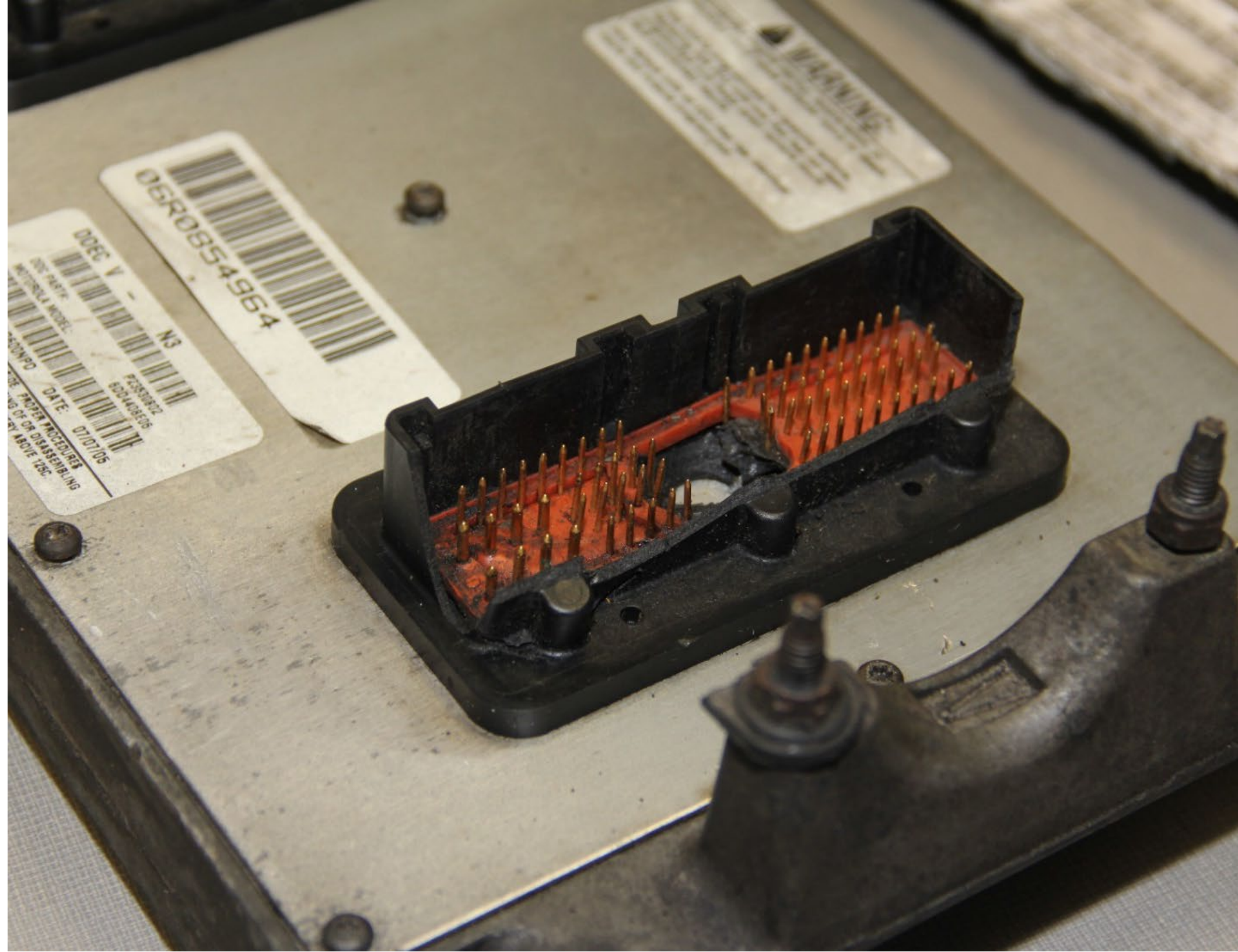




Sometimes the ECU is
Broken



The Recovered Module: No Communications



DDEC Decoding (See SAE 2015-01-1450)

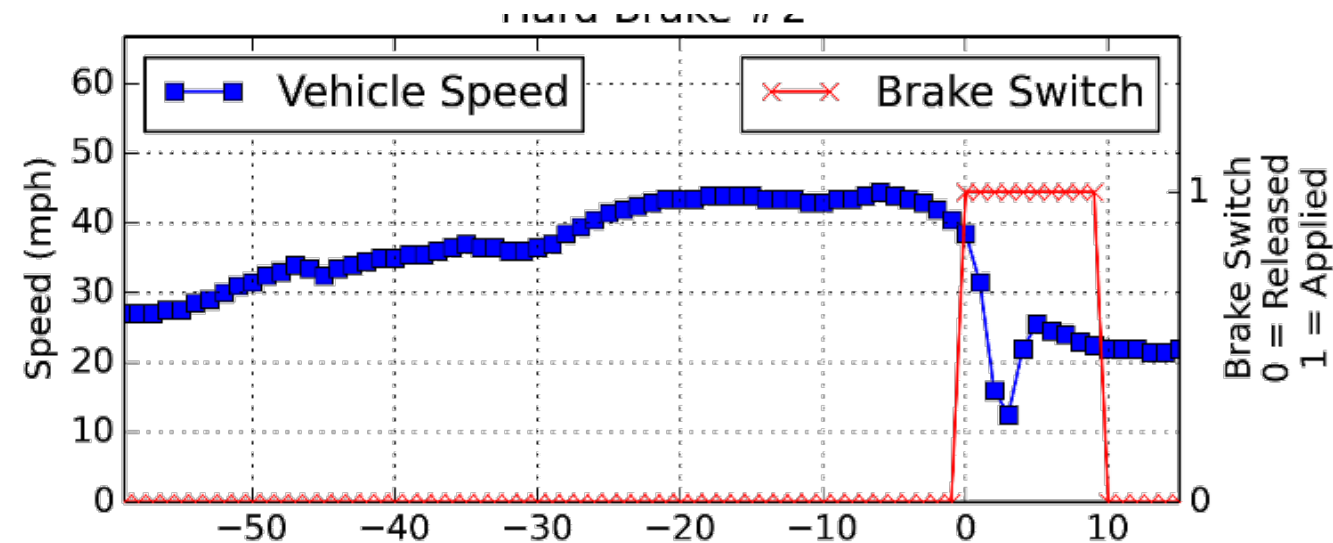
Extracting Event Data from Memory Chips within a Detroit Diesel DDEC V

2015-01-1450
Published 04/14/2015

Jeremy Daily, Andrew Kongs, James Johnson, and Jose Corcega
University of Tulsa

CITATION: Daily, J., Kongs, A., Johnson, J., and Corcega, J., "Extracting Event Data from Memory Chips within a Detroit Diesel DDEC V," SAE Technical Paper 2015-01-1450, 2015, doi:10.4271/2015-01-1450.

Copyright © 2015 SAE International



DDEC Data Decoding Overview

1. Problem definition
2. Figuring out what to look for (Produce Known Data)
3. Locating known data in memory from an exemplar ECM
4. Finding data in the subject ECM (Unknown)
5. Decoding and presenting the data

Normal: DDEC Reports

DDEC® Reports - Hard Brake

#1

Print Date: 10/2/2013 2:30 PM
University of Tulsa

Trip: 09/17/12 12:26:15 To 10/02/13 (CST)
Vehicle ID: DDEC 6 TIB
Driver ID:
Odometer: 619.0 mi
Engine S/N: 06R1003832

Trip Distance	619.0 mi	Trip Time	0:00:00
Trip Fuel	0.00 gal	Fuel Consumption	0.00 gal/h
Fuel Economy	0.00 mpg	Idle Time	0:00:00
Avg Drive Load	0 %	Idle Percent	0.00 %
Avg Vehicle Speed	0.0 mph	Idle Fuel	0.00 gal
		Parked Regen Time	0:00:00

Incident Time: 10/2/2013 1:07:54 PM (CST) Incident Odometer: 619.0 mi

Time	Vehicle Speed (mph)	Engine Speed (rpm)	Brake	Clutch	Engine Load (%)	Throttle (%)	Cruise	Diag. Code
-0:59	23.5	0	No	No	0.00	0.00	No	Yes
-0:58	22.0	0	No	No	0.00	0.00	No	Yes
-0:57	20.0	0	No	No	0.00	0.00	No	Yes
-0:56	18.0	0	No	No	0.00	0.00	No	Yes
-0:55	16.0	0	No	No	0.00	0.00	No	Yes
-0:54	14.0	0	No	No	0.00	0.00	No	Yes
-0:53	12.0	0	No	No	0.00	0.00	No	Yes
-0:52	10.0	0	No	No	0.00	0.00	No	Yes
-0:51	8.0	0	No	No	0.00	0.00	No	Yes
-0:50	6.5	0	No	No	0.00	0.00	No	Yes
-0:49	4.0	0	No	No	0.00	0.00	No	Yes
-0:48	2.5	0	No	No	0.00	0.00	No	Yes
-0:47	1.0	0	No	No	0.00	0.00	No	Yes

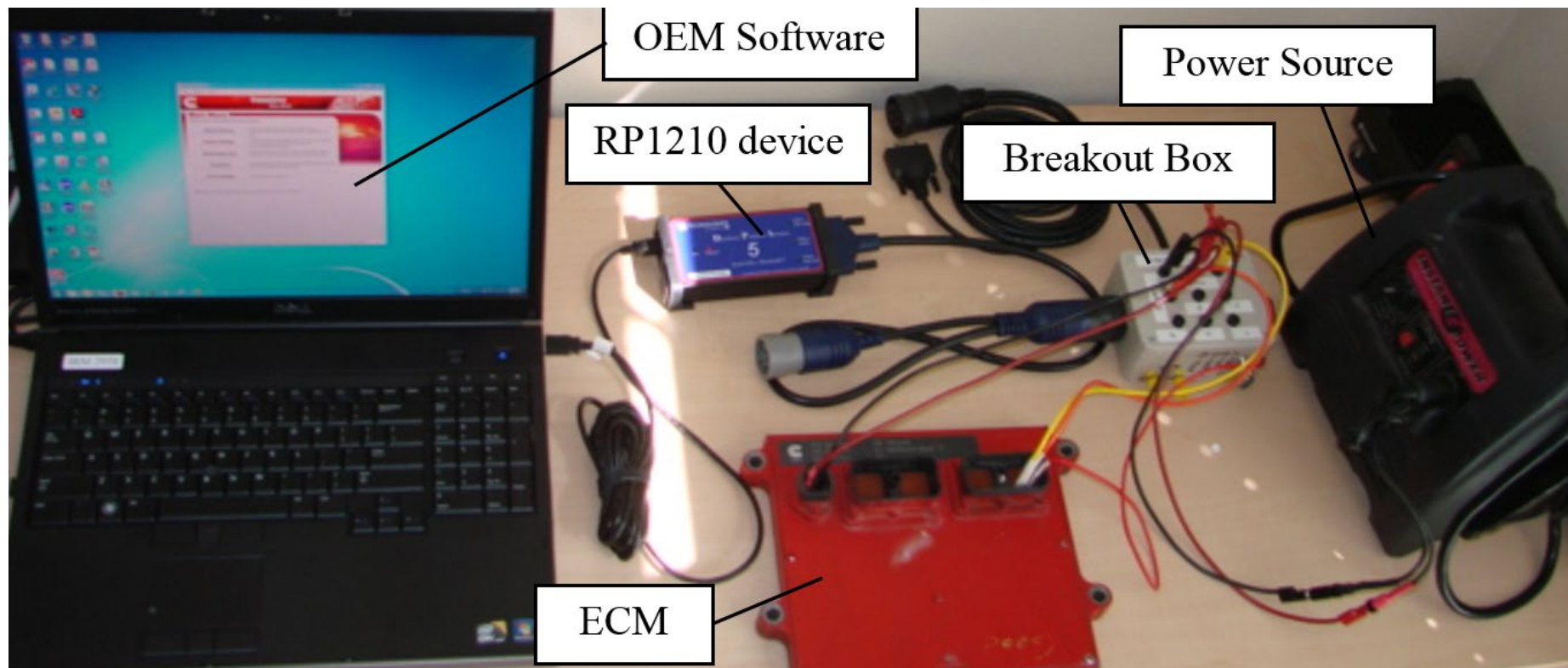
A direct approach may be needed

- The electrical system is compromised.



Bench Top Download (or Image?)

• But this sets new faults.



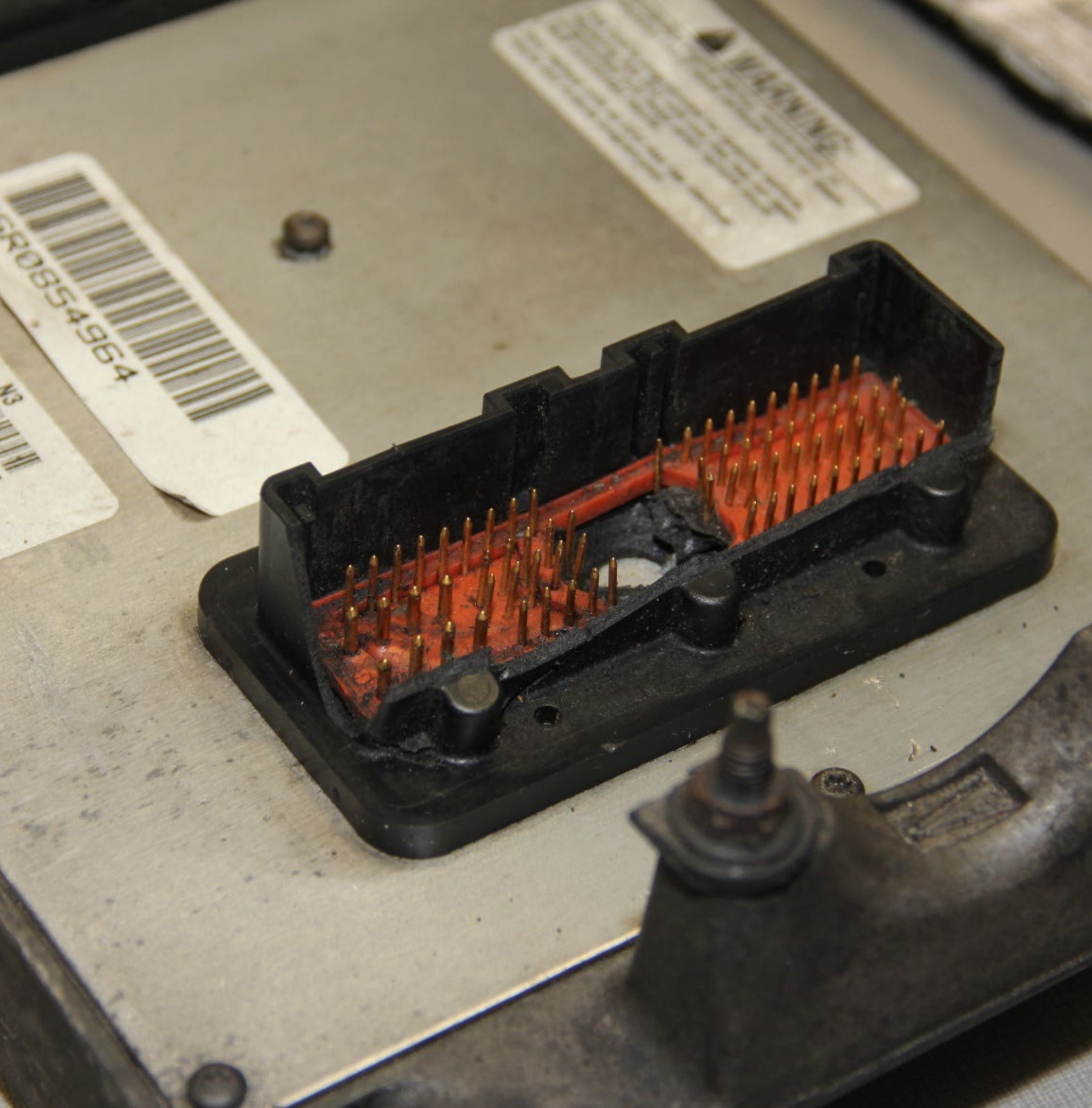
Bench Top Download (Fault Free)



But, sometimes it's not that easy.



The electrical system is compromised.



Attempted Download

- Able to connect, but throws a J1708 Network Error
- This isn't covered in the manual...
- Let's take a peek inside the module.

Gaining Chip Access

- Accessing the chips with a vise and brute force...

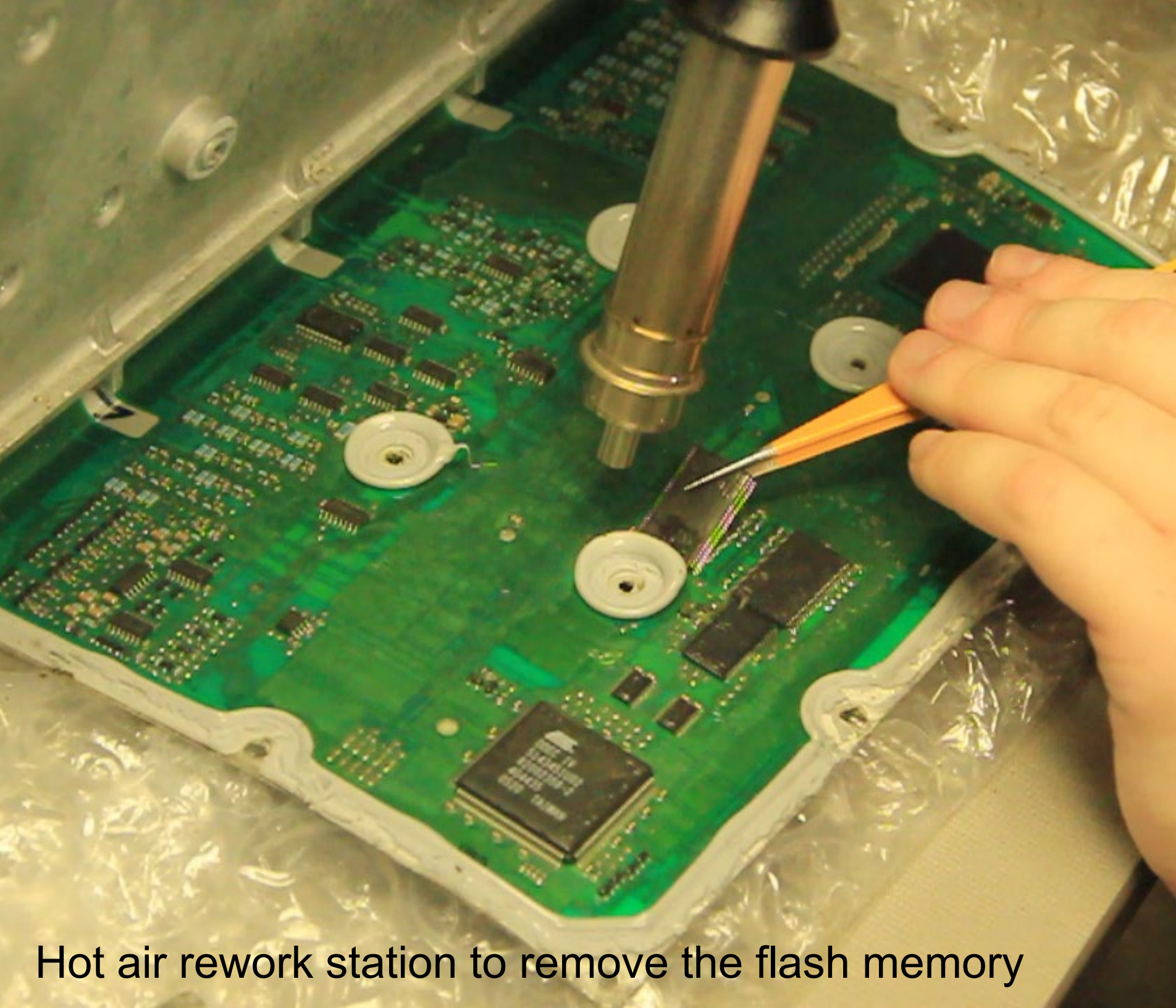




Gaining Chip Access

with a milling machine...





Chip Removal

Hot air rework station to remove the flash memory





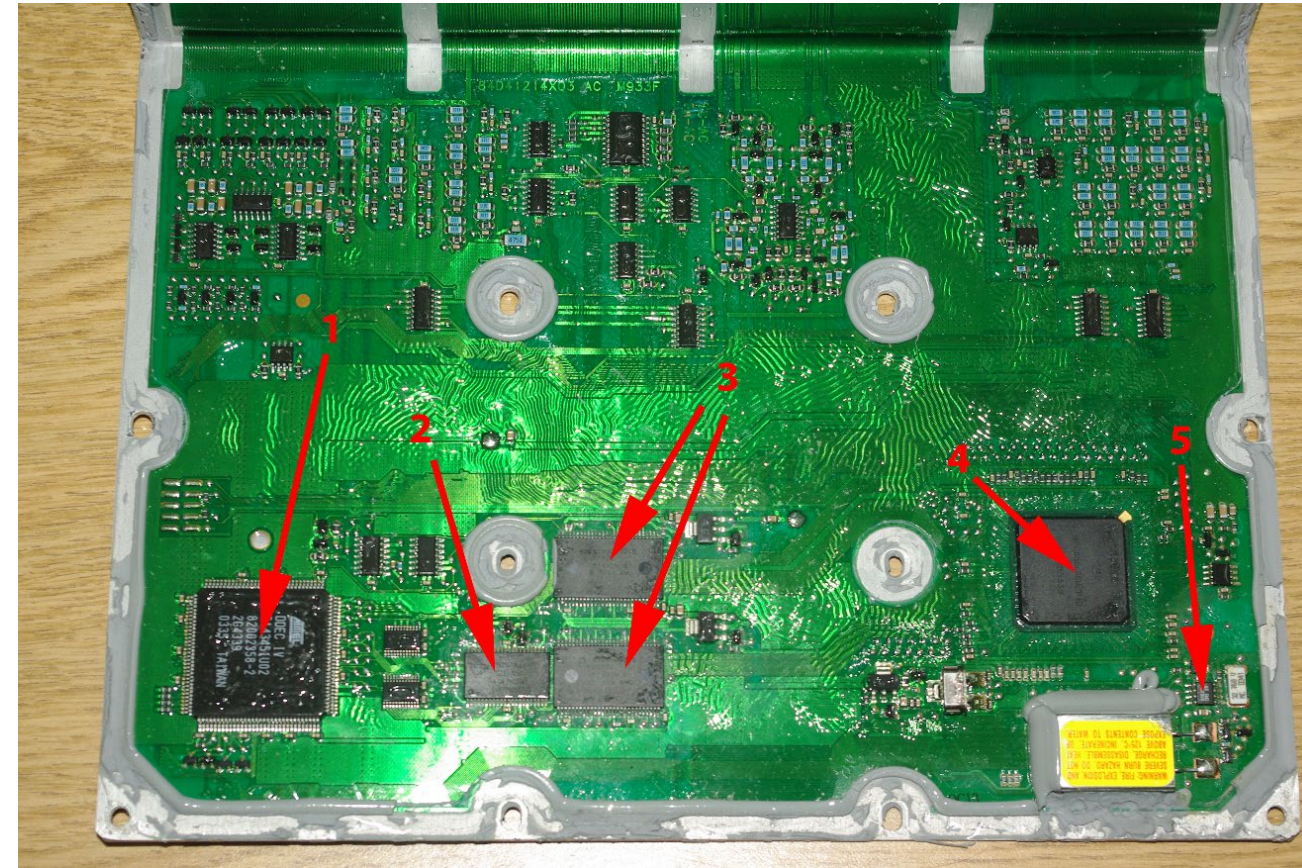
Crash Induced Access

The enclosure is in pieces



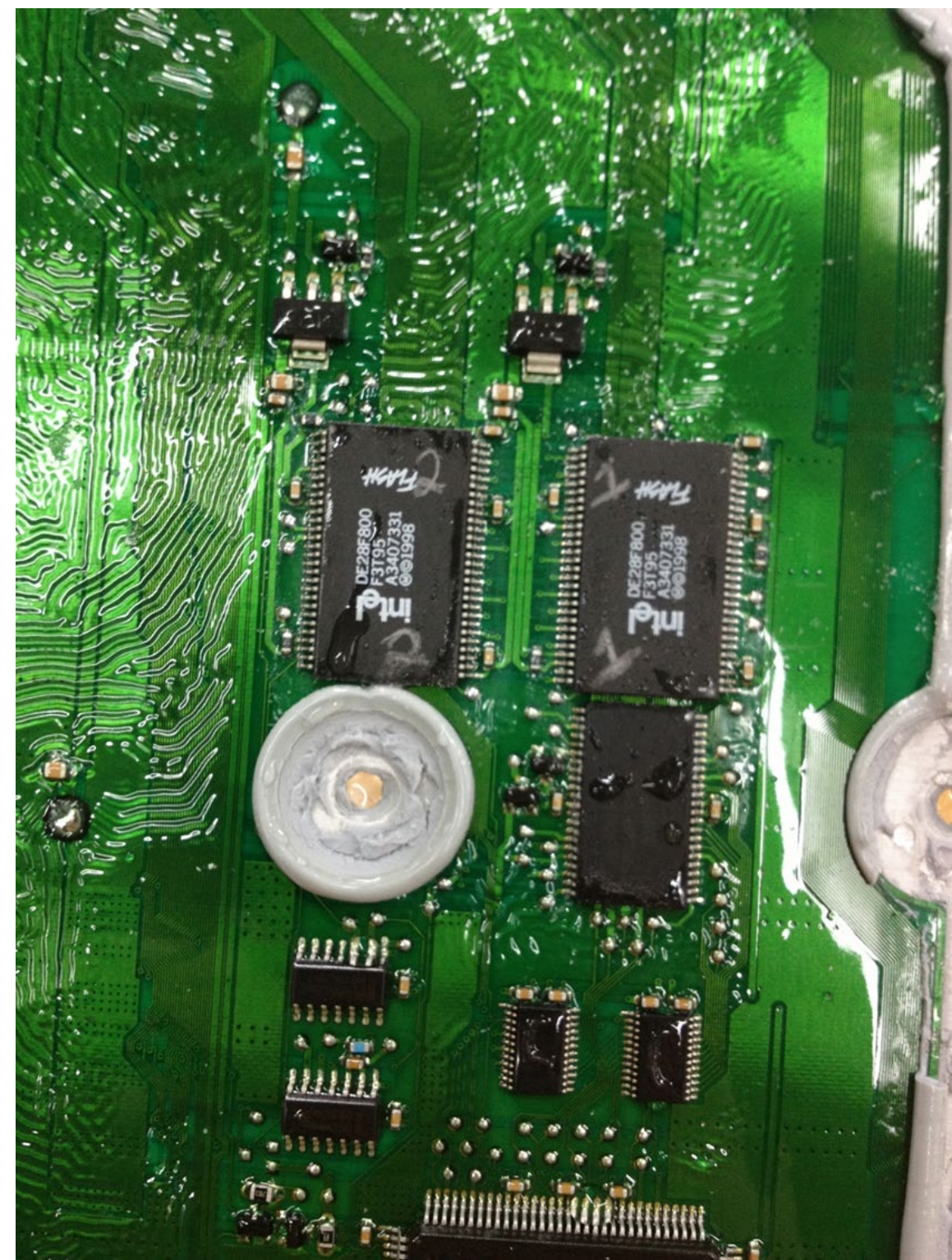
Chip Identification

- DDEC 5
 1. Custom ASIC – similar to later DDEC4
 2. Cypress CY62137VLL SRAM
 3. AMD AM29BL802CB Flash Storage ICs
 4. MPC555LF8MZP40 32-bit CPU
 5. Real-time clock IC EM V3020



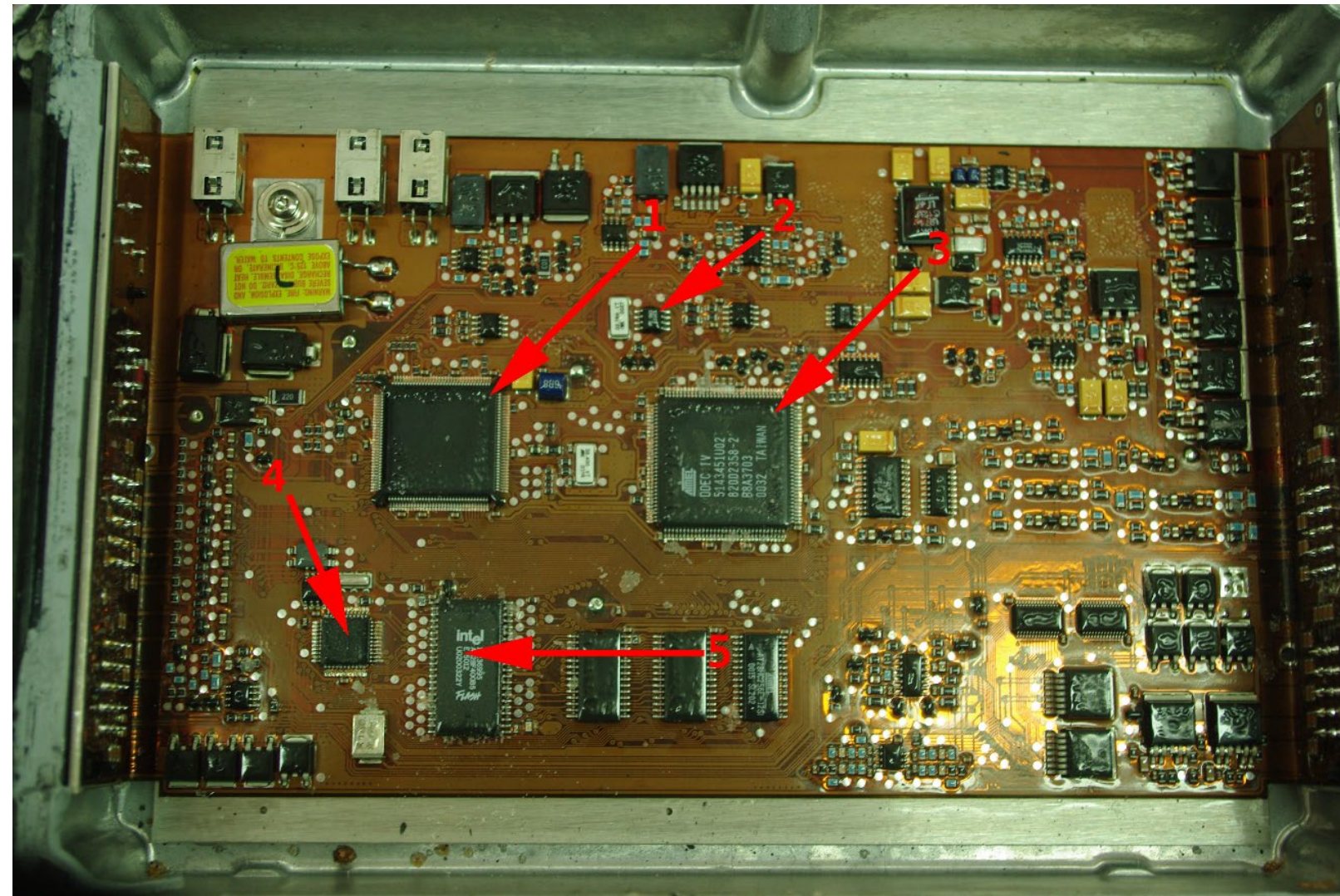
Another DDEC V

- Data is stored on flash memory.
- This DDEC5 used an Intel chip.
- Each chip stores 1 megabyte



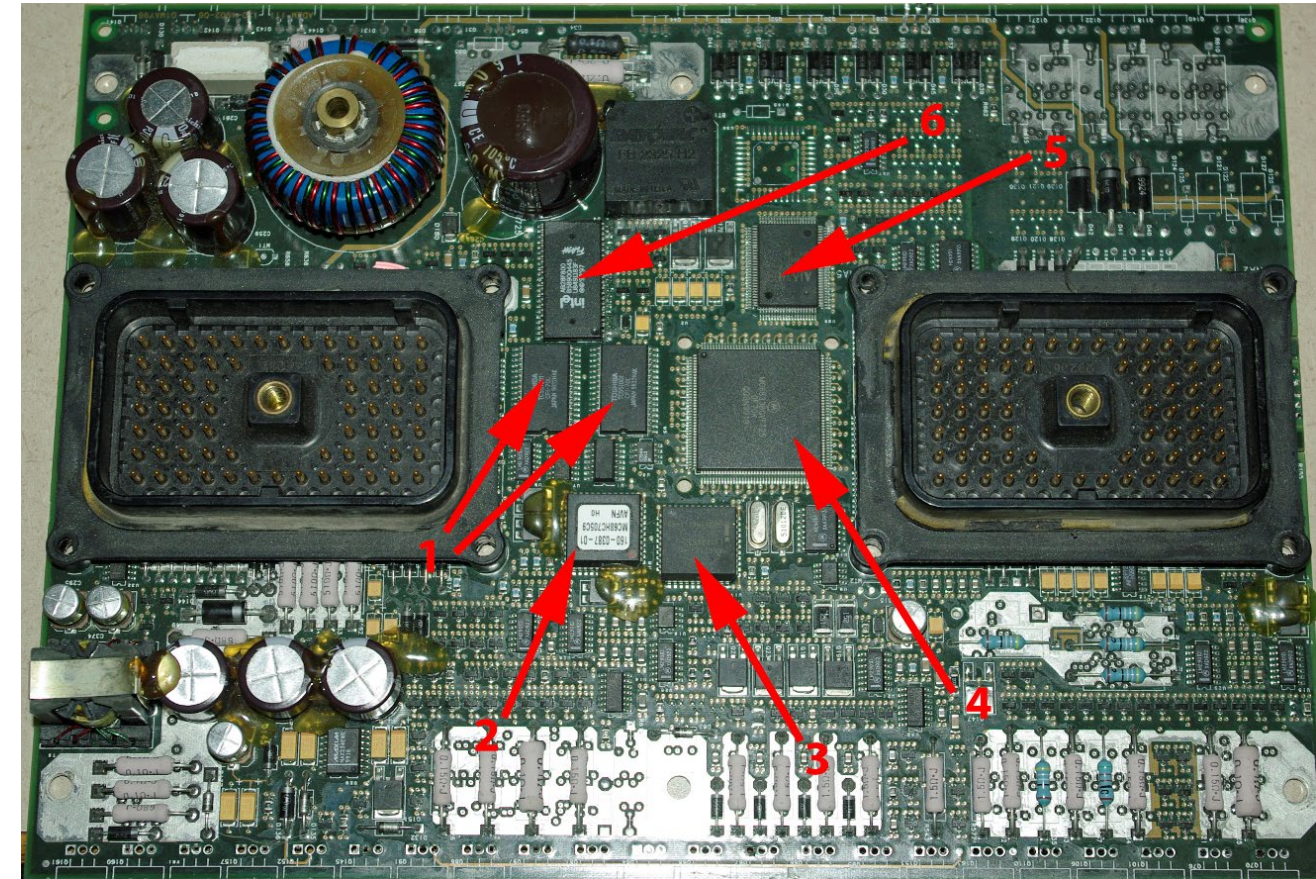
DDEC IV Chip Identification

1. MC68332 – 32-bit CPU
2. Real-time Clock controller
3. Presumed Custom ASIC controller
4. CAN Controller
5. Intel Flash Storage IC AB28F400

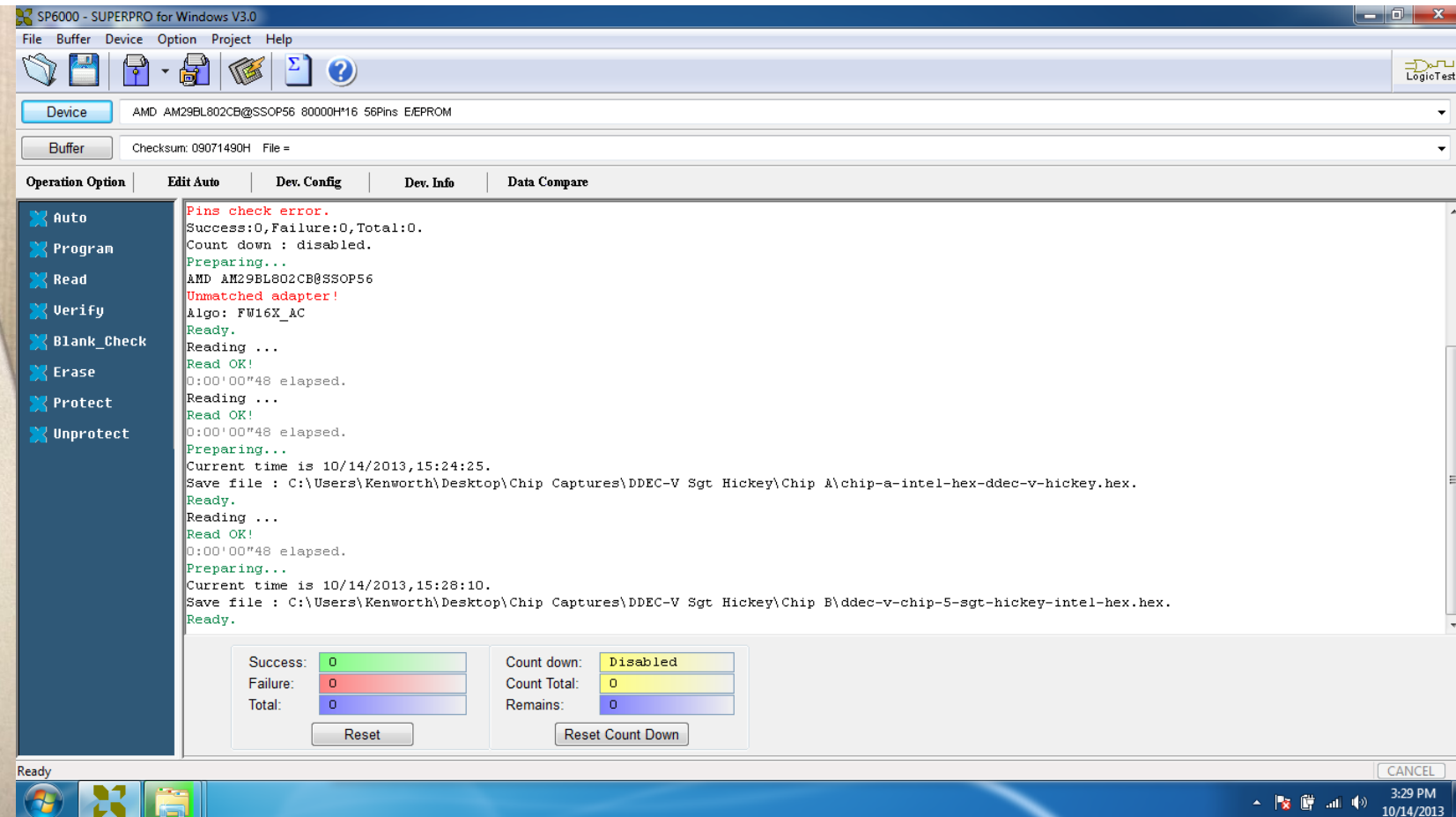


CAT ADEM III Chip Identification

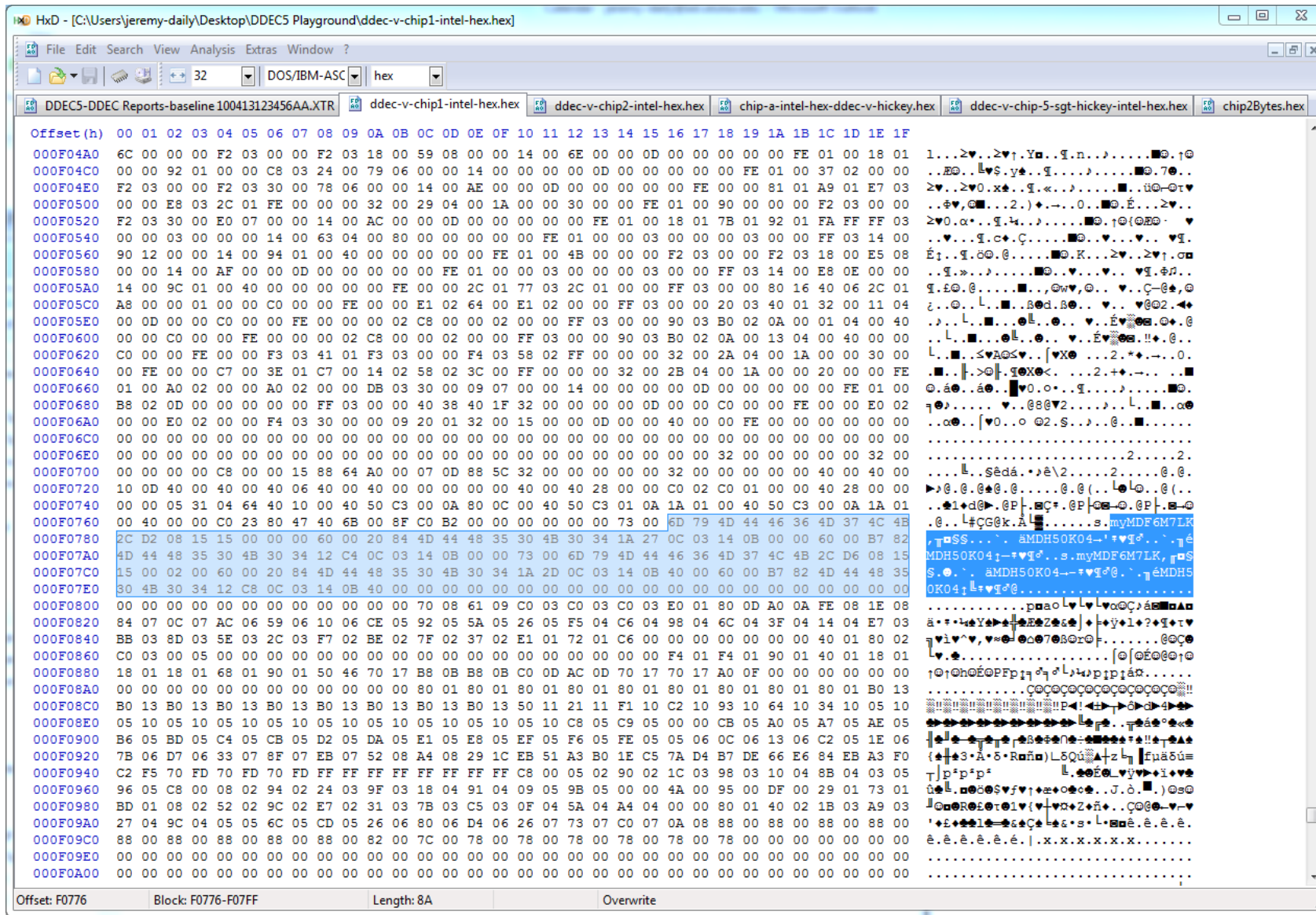
1. Toshiba SRAM
2. MC68HC705C9A 8-bit Microcontroller (EEPROM)
3. Intel CAN 2.0 Controller
4. MC68336 32-bit Microprocessor (note: Mask-ROM + SRAM)
5. AMI IC Branded Caterpillar, Presumed ASIC
6. Intel AB28F800 5V Flash Storage



Reading Memory Chip Contents



Results in a Hex Editor



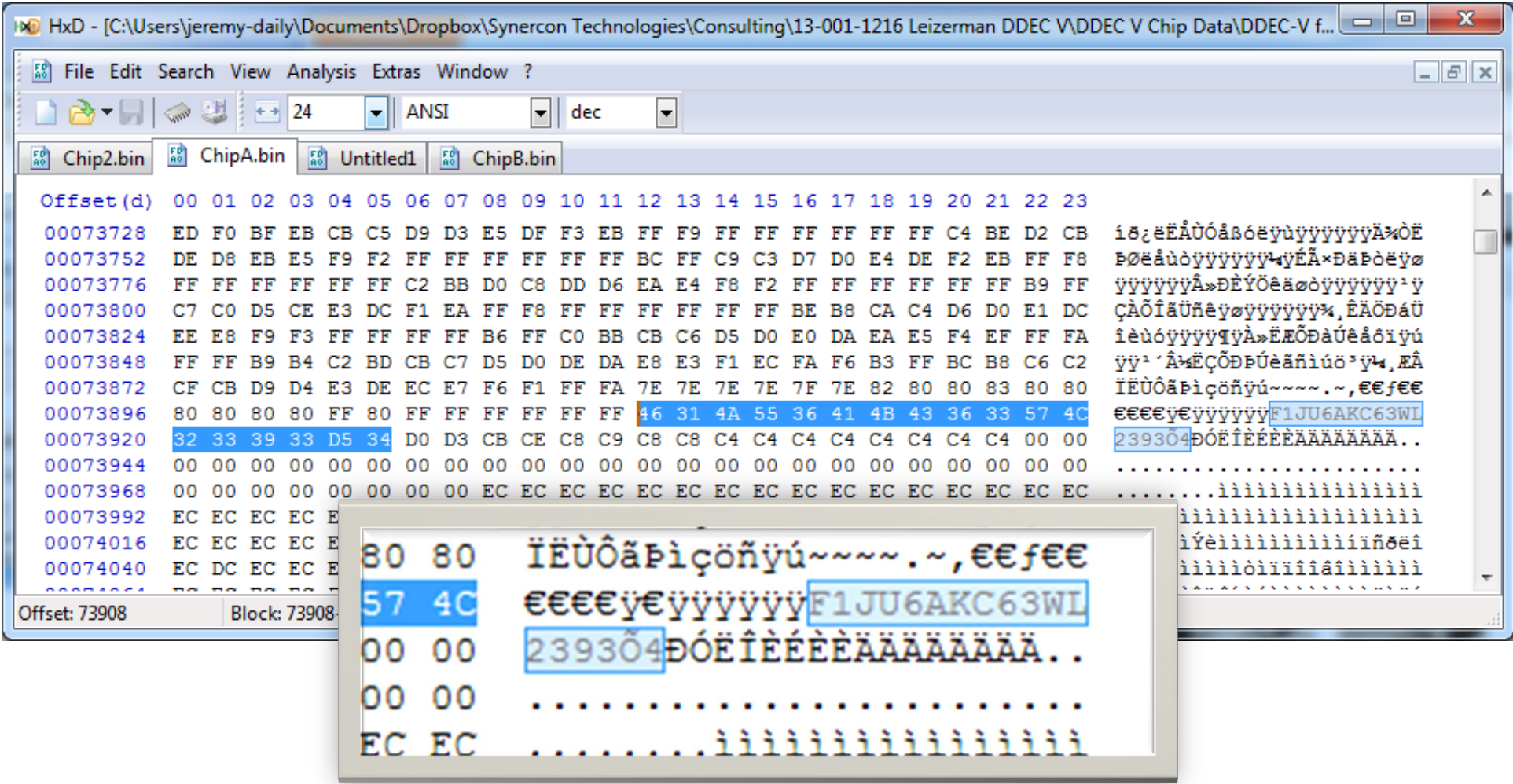
Understanding Hex Data as Powers of 2

Bit position	8	7	6	5	4	3	2	1	Notes
Exponent	7	6	5	4	3	2	1	0	1 less than position
2^Exponent	128	64	32	16	8	4	2	1	Value of the bits
Bits	1	0	0	1	1	1	0	0	Example
Bit values	128	0	0	16	8	4	0	0	156
Nibbles	9				C				Use letters for numbers > 9 Concatenate Nibbles
Byte (hex)	9C								
Decimal	156								

- Hex is base 16 condensed representation of binary (base 2)
- Uses 0-9, A-F to get 16 characters
- Each character is a nibble (4-bits), 2 nibbles is a byte (8-bits)
- All data in computers and networks are represented as binary (1 or 0)

Human Readable Data

Letters and numbers are encoded using ASCII. Look for known ASCII, like VIN and Serial Number.



Hex Data...



Hexadecimal Data

```
B600: 20 50 08 00 00 00 00 00
B608: 00 00 00 00 AA 00 00 00
B610: 00 00 00 00 AA 45 F9 F9
B618: F9 F9 F9 9D F9 F9 FF AA
B620: AA AA 00 00 00 00 00 00
B628: 00 00 00 00 00 00 00 00
B630: 00 00 00 00 00 00 00 00
B638: 00 00 00 00 00 00 00 00
B640: 00 00 00 00 00 00 00 00
B648: 00 00 00 00 00 00 00 00
B650: 00 00 00 00 00 00 00 AA
B658: 00 25 82 20 50 08 00 00
B660: 00 00 00 00 00 00 00 00
B668: 00 00 00 00 00 00 00 00
B670: 00 00 00 00 00 00 00 00
B678: 00 00 00 00 00 00 43 69
B680: 00 00 00 55 AA AA AA AA
B688: 00 00 00 BE 86 00 01 16
B690: 87 00 01 6C 88 00 01 7D
```

Manufacturers specify what the hex data means

Sometimes, manufacturers use standards for the meaning of data

Reverse engineering processes can help decode non-standardized data

Meaning Applied to HVEDRs

- Standards Based Meaning
- SAE J1587

A.84 ROAD SPEED

Indicated vehicle velocity.

Parameter Data Length: 1 Character
Data Type: Unsigned Short Integer
Bit Resolution: 0.805 km/h (0.5 mph)
Maximum Range: 0.0 to 205.2 km/h (0.0 to 127.5 mph)
Transmission Update Period: 0.1 s
Message Priority: 1
Format:

PID	Data
84	a
a—	Road speed

- SAE J1939-71
- SAE J1939-73

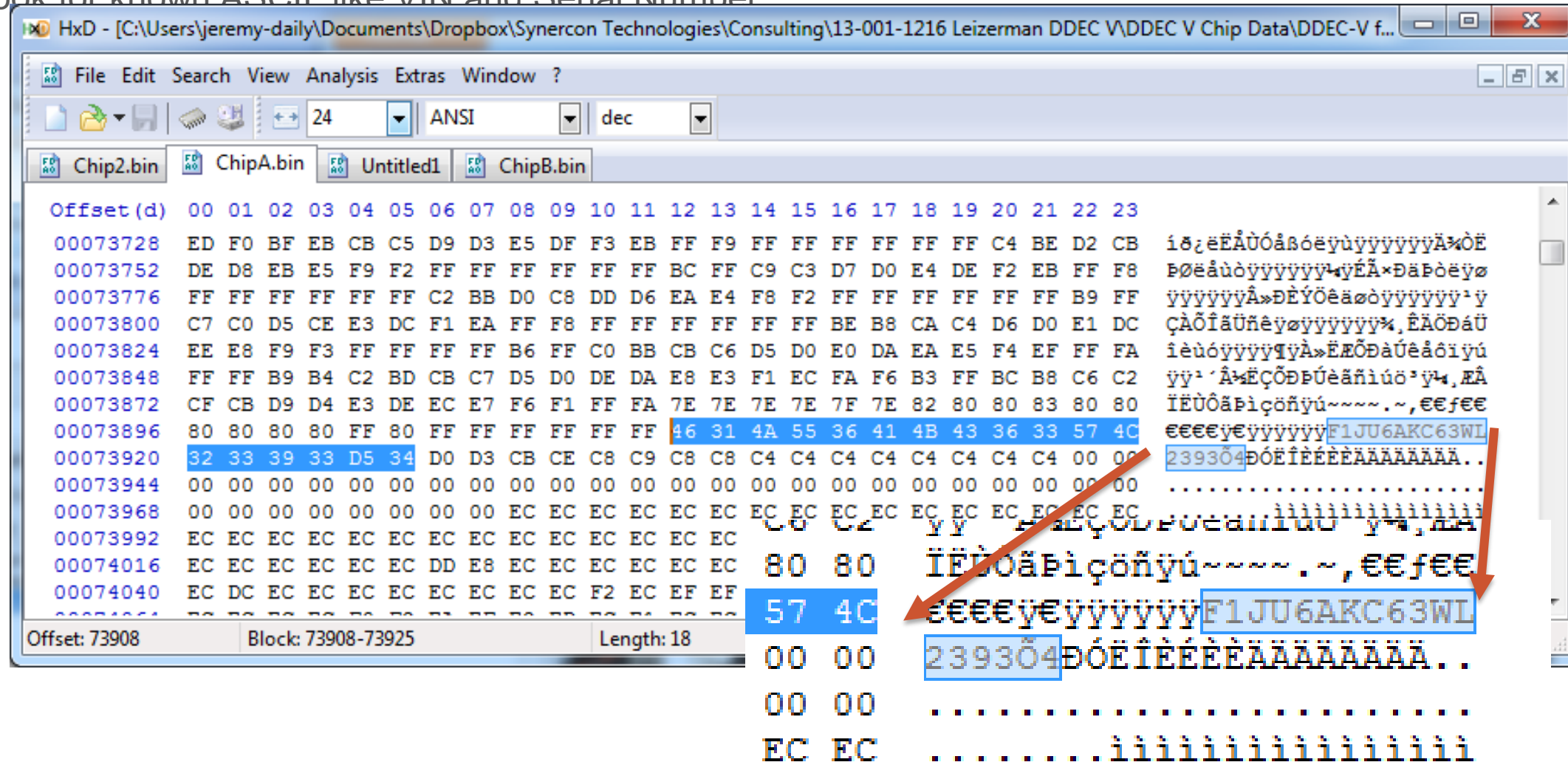
SAE <i>International</i> [™]	SURFACE VEHICLE RECOMMENDED PRACTICE	SAE	J1587 JUL2008
		Issued	1988-01
		Revised	2008-07
		Superseding	J1587 FEB2002
Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications			

SAE <i>International</i> [™]	SURFACE VEHICLE RECOMMENDED PRACTICE	SAE	J1939-71 FEB2010
		Issued	1994-08
		Revised	2010-02
		Superseding	J1939-71 JAN2009
Vehicle Application Layer (Through February 2009)			

Human Readable Hex

- Letters and numbers are encoded using ASCII.

- Strategy: Look for known ASCII like VIN and Serial Number



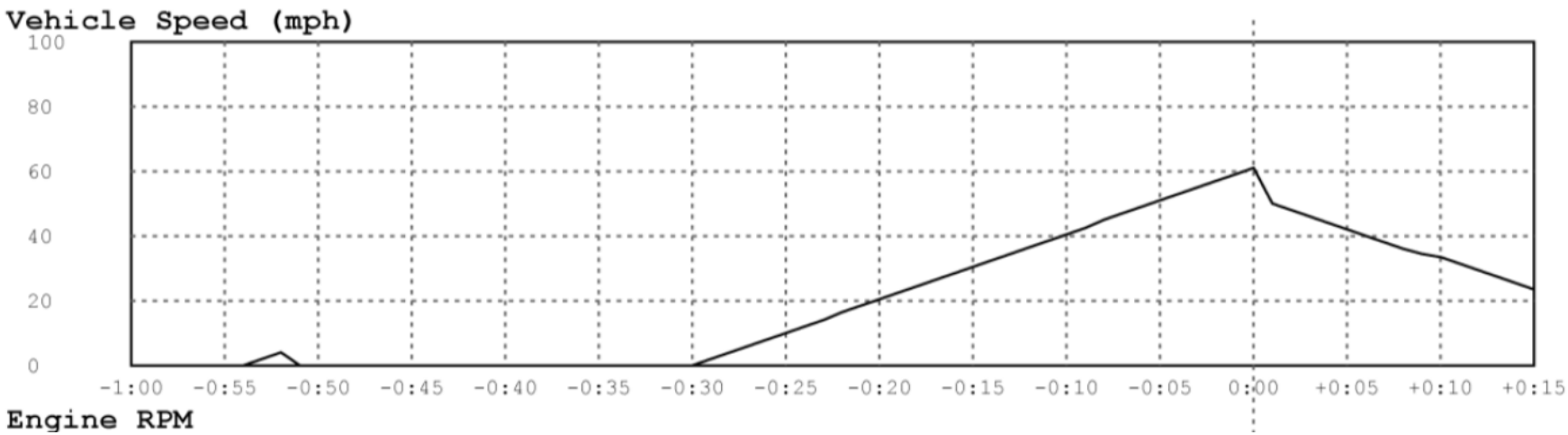
2 Byte Reversals

- The flash memory is used such that the bytes are stored with bytes that are reversed.
 - The VIN from the raw memory says:
 - F1 JU 6A KC 63 WL 23 93 ⬮4
- After swapping every 2 bytes, it becomes:
1FUJA6CK36LW32394
- This is 18 bytes, but VINs are 17 characters
- We can also find serial numbers (search for “R6”)

Simulated Data

- Issue: Still need to decode the data...
- Strategy: Get an exemplar ECM and put a known speed record on it to find the Hard Brake and Last Stop Events.

DDEC® Reports - Hard Brake				#1
Print Date: 10/4/2013 1:23 PM		Trip: 12/12/05 20:56:39 To 10/04/13 (PST)		
DDC		Vehicle ID: DDEC5-TEST		
		Driver ID:		
, -		Odometer: 532323.9 mi		
() -		Engine S/N: 06R0760090		
Trip Distance 473875.7 mi		Trip Time 20869:22:45		
Trip Fuel 94635.50 gal		Fuel Consumption 4.53 gal/h		
Fuel Economy 5.01 mpg		Idle Time 11330:35:08		
Avg Drive Load 46 %		Idle Percent 54.29 %		
Avg Vehicle Speed 49.7 mph		Idle Fuel 7417.38 gal		
Incident Time: 10/04/13 7:14:18 (PST)		Incident Odometer: 532323.0 mi		



Get help from the network logs

- DDEC Reports downloads data in 9 groups called data pages.
- Use J1587 Transport layer to reconstruct the network traffic.
- *.XTR file is close to a network log.
- We can map the XTR file contents to DDEC Reports elements (See SAE 2014-01-0495)
- Enables pattern matching for data elements like Mileage and Times.

Find the patterns (Hard Brake)

Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

00004000 00 00 00 00 00 14 00 51 00 02 FF 07 E7 39 51 00 BA E3 0C 00 1A EC DA 04 66 F2 00 00 77 96 8A 02

00004032 87 02 00 00 89 CB 03 00 46 86 8F 00 00 00 00 00 00 00 00 90 9E 0D 00 2E 17 8A 15 00 8C C6 08

00004064 00 00 00 00 00 B2 45 2E 01 7F C2 2B CA EB 8B 2A 2C A7 CD 28 00 00 00 00 00 00 00 02 00 A8 03 01 7B

00004096 B6 E7 06 00 DE 39 51 00 4B 8F 90 17 36 00 00 00 00 00 60 00 00 00 00 00 60 00 00 00 00 00 60 00

00004128 00 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 60 04 00 00 00 00 60 08 00 00 00 00 60 00 00 00

00004160 00 00 60 00 00 00 00 00 60 00 00 00 00 00 00 00 00 60 00 00 00 00 00 60 00 00 00 00 60 00 00 00

00004192 60 00 00 00 00 00 00 00 60 00 00 00 00 00 00 00 00 60 00 00 00 00 00 60 00 00 00 00 60 00 00 00

00004224 00 00 00 00 60 00 00 00 60 00 00 00 00 00 00 00 00 60 00 00 00 00 00 60 00 00 00 00 60 00 00 00

00004256 00 00 60 00 00 00 00 00 60 00 00 00 00 00 00 00 00 60 00 00 00 00 00 60 00 00 00 00 60 00 00 00

00004288 60 04 00 00 00 00 00 00 60 08 00 00 00 00 60 0C 00 00 00 00 60 10 00 00 00 00 60 14 00 00 00 00 60 18

00004320 00 00 00 00 60 1C 00 00 00 00 60 21 00 00 00 00 60 25 00 00 00 00 60 29 00 00 00 00 60 2D 00 00 00

00004352 00 00 60 31 00 00 00 00 60 35 00 00 00 00 60 39 00 00 00 00 60 3D 00 00 00 00 60 41 00 00 00 00 60

00004384 60 45 00 00 00 00 00 00 60 49 00 00 00 00 60 4D 00 00 00 00 60 51 00 00 00 00 60 55 00 00 00 00 60 5A

00004416 00 00 00 00 60 5E 00 00 00 00 60 62 00 00 00 00 60 66 00 00 00 00 60 6A 00 00 00 00 60 6E 00 00 00

00004448 00 00 60 72 00 00 00 00 60 76 00 00 00 00 60 7A 00 00 00 00 60 7E 00 00 00 00 60 82 00 00 00 00 60

00004480 60 5C 00 00 00 00 00 00 60 58 00 00 00 00 60 54 00 00 00 00 60 50 00 00 00 00 60 4C 00 00 00 00 60 48

00004512 00 00 00 00 60 45 00 00 00 00 60 43 00 00 00 00 60 3F 00 00 00 00 60 3B 00 00 00 00 60 37 00 00 00

00004544 00 00 60 33 00 00 00 00 60 2F 00 00 00 00 60 CA 90 17 36 68 96 06 00 4A BB 4D 00 4B B4 12 9D 2E

00004576 36 6E 17 30 65 40 36 75 17 28 5E 40 36 67 17 2A 60 40 37 A1 17 35 6B 40 37 CE 17 37 6B 40 39 61

00004608 18 50 83 40 3A FE 18 51 84 40 3C B7 19 51 85 40 3E 7A 1A 61 93 40 3F 2A 1B 5E 90 40 41 FC 1B 5A

00004640 8F 40 42 A5 1C 59 8E 40 44 1C 1D 5B 8F 40 43 6A 14 00 00 40 41 B7 10 3D 5D 40 43 83 14 4B 78 40

00004672 44 D8 14 51 7D 40 45 20 15 52 7D 40 46 76 15 50 7D 40 46 7B 15 34 63 40 47 C7 15 4E 7D 40 47 0A

00004704 16 4B 7B 40 48 3A 16 4A 7B 40 49 8F 16 52 82 40 4A C3 16 3F 73 40 49 9A 16 1B 3E 40 49 7A 16 15

00004736 2F 40 48 0D 16 14 2E 40 48 23 16 40 73 40 49 5C 16 4A 7B 40 4A CF 16 67 A0 40 4D 9A 17 80 AA 40

00004768 4F 49 18 7E A8 40 51 F2 18 73 A1 40 53 9A 19 71 9F 40 54 07 1A 61 94 40 55 65 1A 5A 8D 40 56 93

00004800 1A 53 86 40 57 B2 1A 37 70 40 57 DD 1A 47 7D 40 57 F6 1A 40 79 40 58 0E 1B 41 7A 40 58 28 1B 3D

00004832 76 40 58 35 1B 38 71 40 58 16 1B 2B 63 40 57 E2 1A 26 5E 40 57 DC 1A 2B 63 40 57 C9 1A 30 68 40

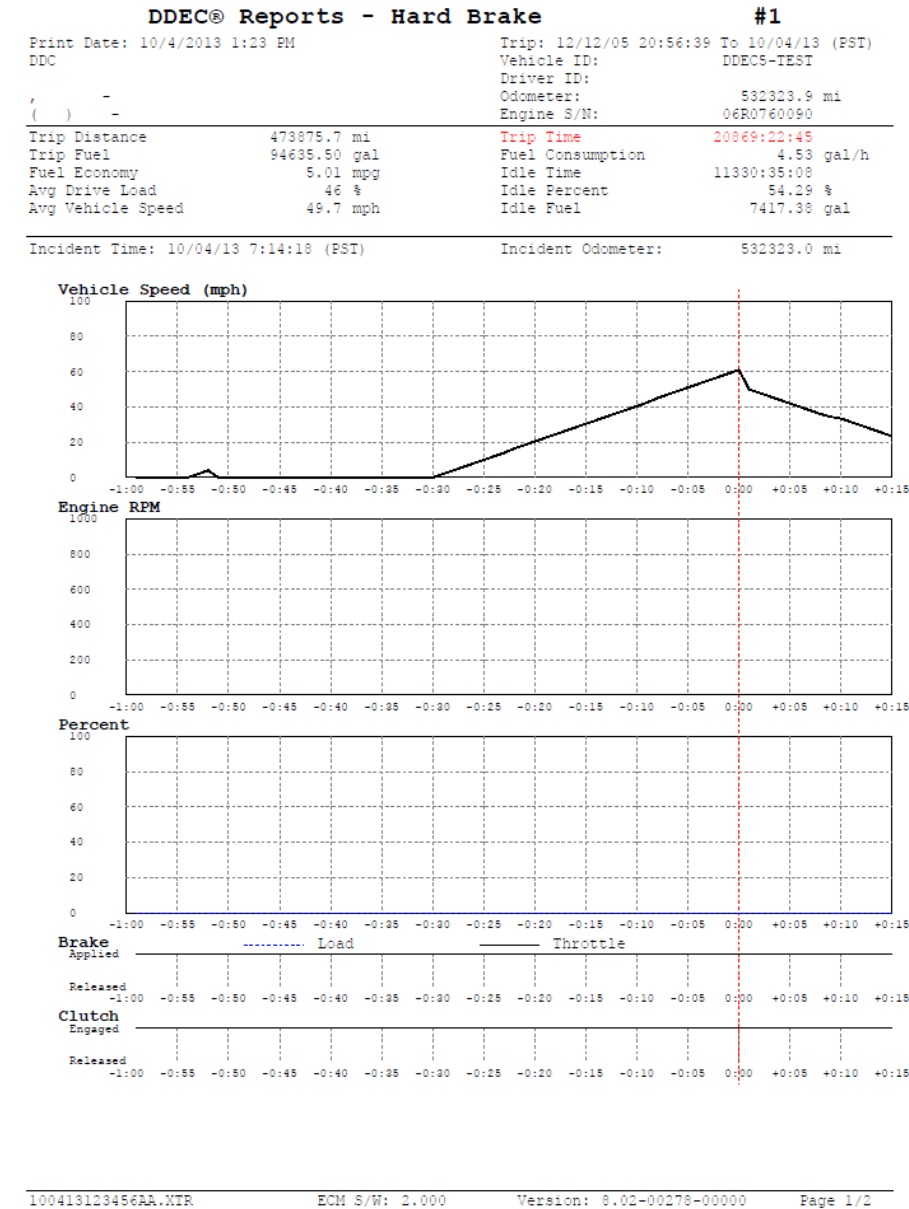
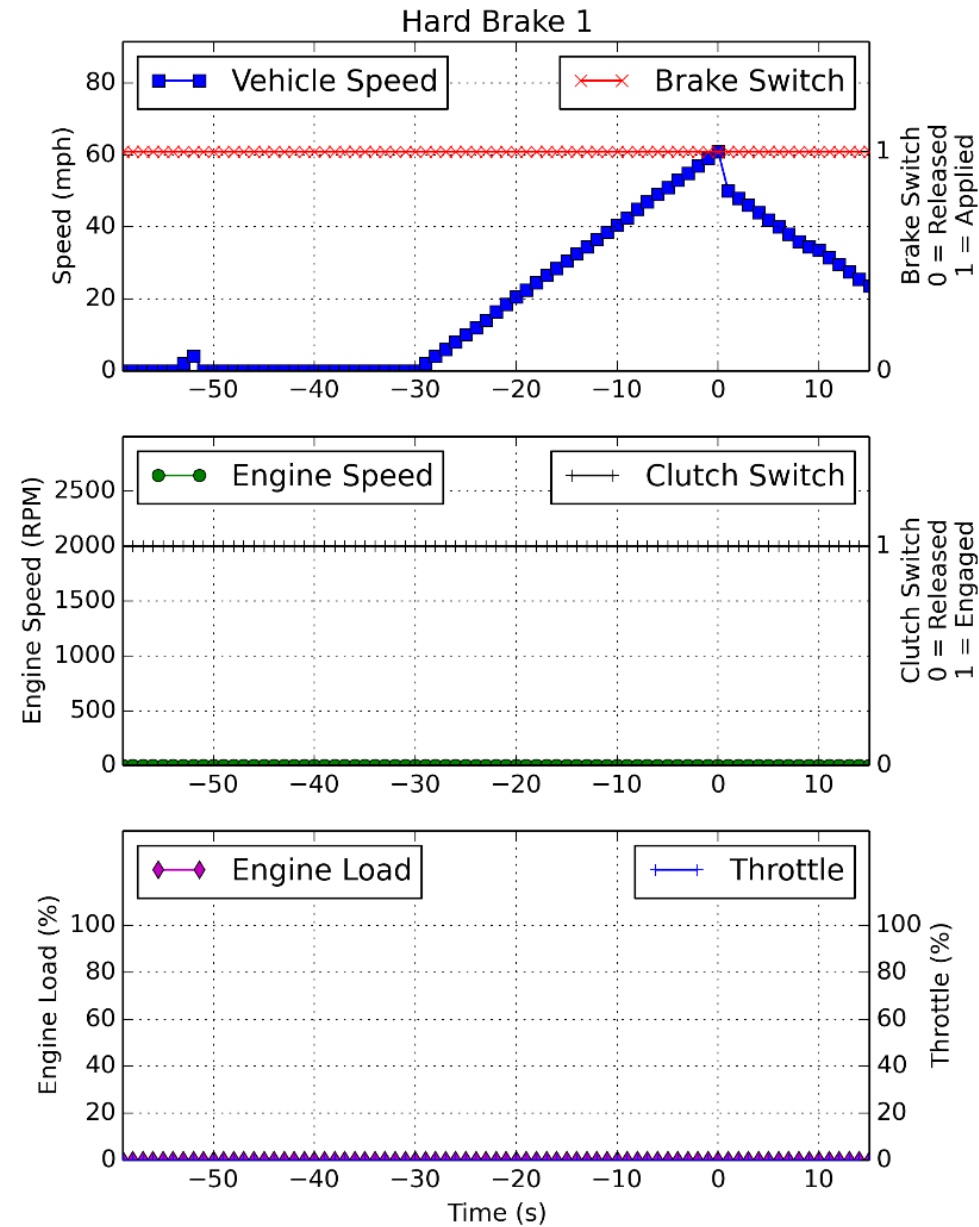
00004864 56 91 14 00 00 40 56 11 13 5A 9D 40 57 39 13 5D 80 40 57 58 13 58 7D 40 58 92 13 65 87 40 59 B2

Last Stop Data

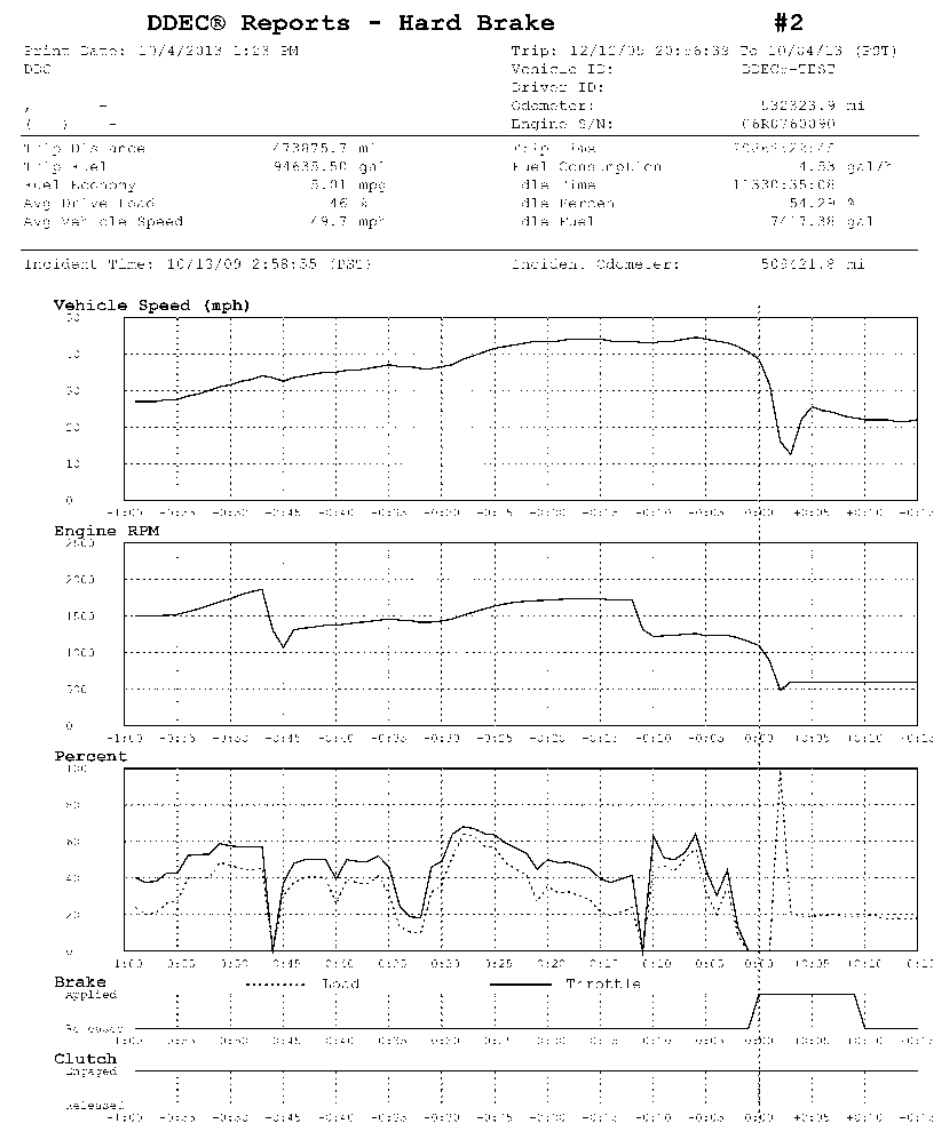
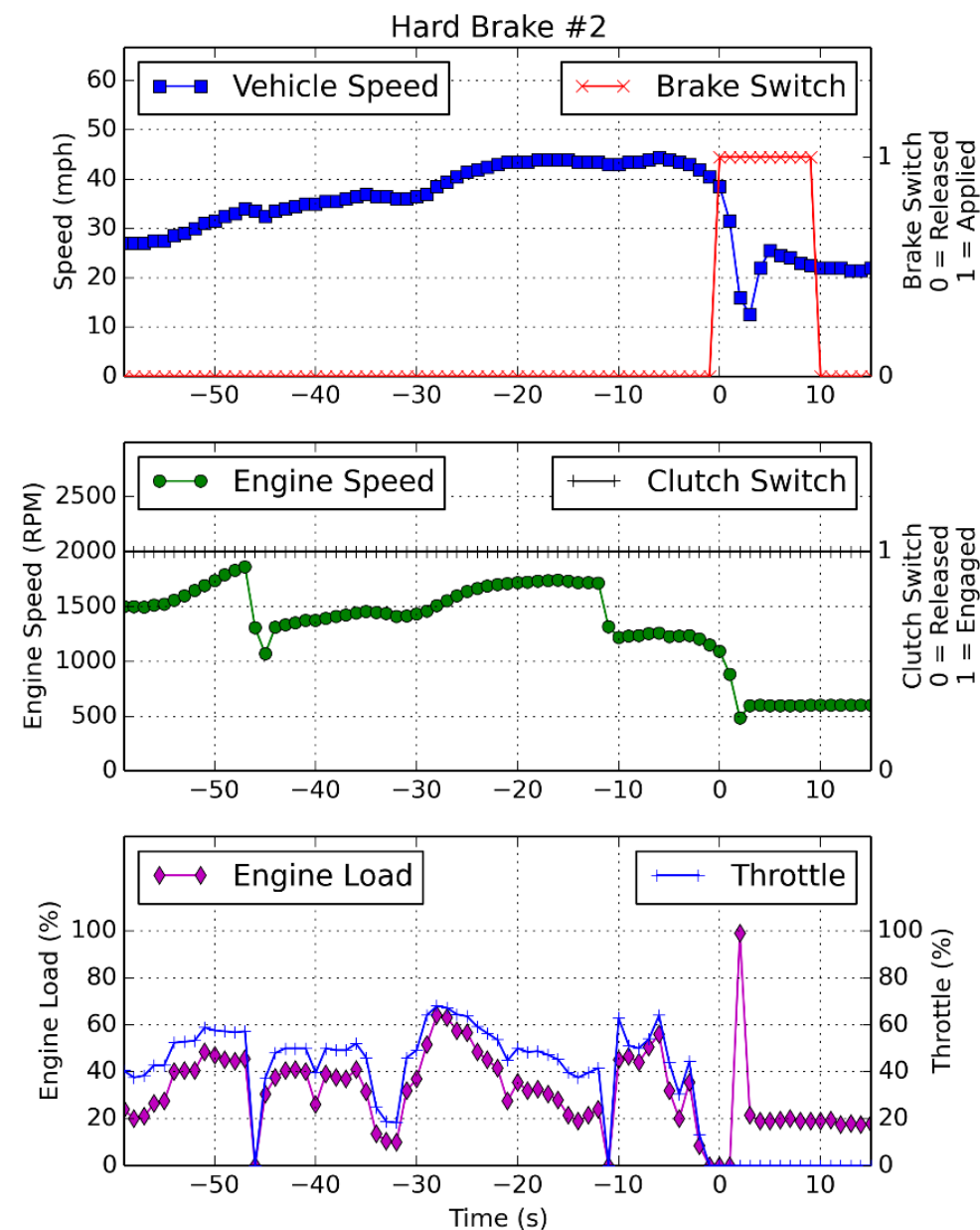
00868800 60 00 00 00 00 1C 60 00 00 00 00 21 60 00 00 00 00 25 60 00 00 00 00 29 60 00 00 00 00 2D 60 00
00868832 00 00 00 31 60 00 00 00 00 35 60 00 00 00 39 60 00 00 00 3D 60 00 00 00 41 60 00 00 00
00868864 00 45 60 00 00 00 00 49 60 00 00 00 4D 60 00 00 00 51 60 00 00 00 55 60 00 00 00 5A
00868896 60 00 00 00 00 5E 60 00 00 00 62 60 00 00 00 66 60 00 00 00 6A 60 00 00 00 6E 60 00
00868928 00 00 00 72 60 00 00 00 76 60 00 00 00 7A 60 00 00 00 7E 60 00 00 00 82 60 00 00 00
00868960 00 5C 60 00 00 00 58 60 00 00 00 54 60 00 00 00 50 60 00 00 00 4C 60 00 00 00 48
00868992 60 00 00 00 00 45 60 00 00 00 43 60 00 00 00 3F 60 00 00 00 3B 60 00 00 00 37 60 00
00869024 00 00 00 33 60 00 00 00 2F 60 00 00 00 DA 04 1A EC 4E 14 A9 77 17 36 CA 90 17 36 8F 90 00 4B
00869056 00 00 7C D1 6E 17 30 36 40 65 75 17 28 36 40 5E 67 17 2A 36 40 60 A1 17 35 37 40 6B CE 17 37 37
00869088 40 6B 61 18 50 39 40 83 FE 18 51 3A 40 84 B7 19 51 3C 40 85 7A 1A 61 3E 40 93 2A 1B 5E 3F 40 90
00869120 FC 1B 5A 41 40 8F A5 1C 59 42 40 8E 1C 1D 5B 44 40 8F 6A 14 00 43 40 00 B7 10 3D 41 40 5D 83 14
00869152 4B 43 40 78 D8 14 51 44 40 7D 20 15 52 45 40 7D 76 15 50 46 40 7D 7B 15 34 46 40 63 C7 15 4E 47
00869184 40 7D 0A 16 4B 47 40 7B 3A 16 4A 48 40 7B 8F 16 52 49 40 82 C3 16 3F 4A 40 73 9A 16 1B 49 40 3E
00869216 7A 16 15 49 40 2F 0D 16 14 48 40 2E 23 16 40 48 40 73 5C 16 4A 49 40 7B CF 16 67 4A 40 A0 9A 17
00869248 80 4D 40 AA 49 18 7E 4F 40 A8 F2 18 73 51 40 A1 9A 19 71 53 40 9F 07 1A 61 54 40 94 65 1A 5A 55
00869280 40 8D 93 1A 53 56 40 86 B2 1A 37 57 40 7D DD 1A 47 57 40 7D F6 1A 40 57 40 79 0E 1B 41 58 40 7A
00869312 28 1B 3D 58 40 76 35 1B 38 58 40 71 16 1B 2B 58 40 63 E2 1A 26 57 40 5E DC 1A 2B 57 40 63 C9 1A
00869344 30 57 40 68 91 14 00 56 40 00 11 13 5A 56 40 9D 39 13 5D 57 40 80 58 13 58 57 40 7D 92 13 65 58
00869376 40 87 B2 13 70 59 40 A0 35 13 40 58 40 6E 3C 13 28 57 40 4C 50 13 47 56 40 6F CF 12 11 54 40 21
00869408 FB 11 00 51 40 00 1C 11 00 4D 60 00 CD 00 00 3F 60 00 97 07 C6 20 60 00 55 09 2B 19 60 00 5C 09
00869440 26 2C 60 00 58 09 26 33 60 00 58 09 27 31 60 00 58 09 28 30 60 00 5A 09 26 2E 60 00 60 09 26 2D
00869472 60 00 60 09 26 2C 40 00 5E 09 27 2C 40 00 61 09 23 2C 40 00 5E 09 24 2B 40 00 5E 09 23 2B 40 00
00869504 5B 09 24 2C 40 00 00 00 A1 04 23 C1 6E 13 87 D2 9D 2E EF 12 9D 2E B4 12 00 4B 00 62 E8 00 00
00869536 00 00 40 00 00 00 00 40 00 00 00 00 40 00 00 00 00 40 00 00 00 40 00 00 00 40 00 00 00 40 00 00 00
00869568 00 00 B3 0D 42 00 40 00 AA 0D 42 00 40 00 8F 0D 43 40 00 86 0D 43 00 82 0D 40 00 40 00 00 00 40 00
00869600 7A 0D 3F 00 40 00 71 0D 3F 00 40 00 61 0D 40 00 40 00 86 0D 3C 02 40 00 52 0D 40 04 00 00 46 0D
00869632 40 05 00 00 48 0D 3C 05 40 00 3F 0D 3D 06 40 00 41 0D 39 06 40 00 37 0D 3C 06 40 00 38 0D 3A 06
00869664 40 00 37 0D 3B 07 40 00 37 0D 3C 07 60 00 35 0D 3C 07 40 00 32 0D 3C 06 40 00 35 0D 3C 05 40 08
00869696 00 0C 8A 07 40 00 45 0D 4B 08 40 0F FC 0E 59 09 00 61 24 13 4F 0C 00 80 36 16 46 0E 00 77 85 16
00869728 3E 0E 00 70 95 14 25 00 00 4B EC 0F 0C 00 00 9B 0D 64 0C 00 5B C3 10 56 0E 00 7B B6 12 4E 10
00869760 00 84 36 14 4B 11 00 74 4A 15 47 12 00 75 76 15 3D 12 00 6D F4 14 35 12 00 65 6B 14 38 12 00 65
00869792 00 14 38 11 00 64 CB 13 3B 11 00 66 E0 13 3F 11 00 69 F0 13 3C 11 00 68 EF 13 3B 11 00 67 2C 14
00869824 00 00 64 2B 14 38 11 00 64 17 14 38 11 00 64 EB 13 31 11 00 5E 35 14 32 11 00 5F 1A 14 2F 11
00869856 00 13 31 11 00 5B 69 13 31 11 00 5B 87 12 2E 10 00 53 6B 12 3B 10 00 62 10 13 48 10 00 6F
00869888 00 00 69 CD 13 3C 11 00 67 F0 14 3F 12 00 6D 82 15 3C 12 00 6A CB 15 39 13 00 6A 1B 16
00869920 00 16 37 13 00 6B 10 17 38 14 00 6B 96 17 3F 14 00 74 17 18 3D 15 00 72 E4 17 38 14
00869952 00 14 00 5E D1 16 36 14 00 6A 75 16 2F 13 00 61 54 16 35 13 00 68 8A 15 2B 13 00 5B
00869984 00 02 04 14 21 11 00 40 76 12 23 10 00 3F BC 10 2B 0E 00 3E 37 0F 36 0D 00 3F B1 0C
00870016 00 31 09 40 00 C1 0C 31 08 40 00 BD 0C 34 08 40 00 9C 0C 66 09 40 00 CF 0C 31 0B
00870048 00 40 00 B0 0C 37 09 40 00 BB 0C 35 09 40 00 B3 0C 32 08 40 00 B6 0C 33 07 40 00
00870080 00 A6 0C 36 04 60 00 AE 0C 32 00 60 00 A5 0C 35 00 60 00 96 0C 38 00 60 00 AD 0C
00870112 00 38 00 40 00 8E 0C 3E 00 00 93 0C 3C 00 00 95 0C 39 00 00 8D 0C 3B 00
00870144 00 00 00 91 0C 35 00 00 FF 05 0C 38 00 00 53 01 A5 00 00 00 CF 00 A5 00 00
00870176 00
00870208 00
00870240 00
00870272 00
00870304 00
00870336 00
00870368 00
00870400
00870432 00
00870464 00
00870496 00
00870528 00
00870560 00
00870592 00

00869534 00869536 00869538 00869540 00869542 00869544 00869546 00869548 00869550 00869552 00869554 00869556 00869558 00869560 00869562 00869564 00869566 00869568 00869570 00869572 00869574 00869576 00869578 00869580 00869582 00869584 00869586 00869588 00869590 00869592 00869594 00869596 00869598 00869600 00869602 00869604 00869606 00869608 00869610 00869612 00869614 00869616 00869618 00869620 00869622 00869624 00869626 00869628 00869630 00869632 00869634 00869636 00869638 00869640 00869642 00869644 00869646 00869648 00869650 00869652 00869654 00869656 00869658 00869660 00869662 00869664 00869666 00869668 00869670 00869672 00869674 00869676 00869678 00869680 00869682 00869684 00869686 00869688 00869690 00869692 00869694 00869696 00869698 00869700 00869702 00869704 00869706 00869708 00869710 00869712 00869714 00869716 00869718 00869720 00869722 00869724 00869726 00869728 00869730 00869732 00869734 00869736 00869738 00869740 00869742 00869744 00869746 00869748 00869750 00869752 00869754 00869756 00869758 00869760 00869762 00869764 00869766 00869768 00869770 00869772 00869774 00869776 00869778 00869780 00869782 00869784 00869786 00869788 00869790 00869792 00869794 00869796 00869798 00869800 00869802 00869804 00869806 00869808 00869810 00869812 00869814 00869816 00869818 00869820 00869822 00869824 00869826 00869828 00869830 00869832 00869834 00869836 00869838 00869840 00869842 00869844 00869846 00869848 00869850 00869852 00869854 00869856 00869858 00869860 00869862 00869864 00869866 00869868 00869870 00869872 00869874 00869876 00869878 00869880 00869882 00869884 00869886 00869888 00869890 00869892 00869894 00869896 00869898 00869900 00869902 00869904 00869906 00869908 00869910 00869912 00869914 00869916 00869918 00869920 00869922 00869924 00869926 00869928 00869930 00869932 00869934 00869936 00869938 00869940 00869942 00869944 00869946 00869948 00869950 00869952 00869954 00869956 00869958 00869960 00869962 00869964 00869966 00869968 00869970 00869972 00869974 00869976 00869978 00869980 00869982 00869984 00869986 00869988 00869990 00869992 00869994 00869996 00869998 00870000 00870002 00870004 00870006 00870008 00870010 00870012 00870014 00870016 00870018 00870020 00870022 00870024 00870026 00870028 00870030 00870032 00870034 00870036 00870038 00870040 00870042 00870044 00870046 00870048 00870050 00870052 00870054 00870056 00870058 00870060 00870062 00870064 00870066 00870068 00870070 00870072 00870074 00870076 00870078 00870080 00870082 00870084 00870086 00870088 00870090 00870092 00870094 00870096 00870098 00870100 00870102 00870104 00870106 00870108 00870110 00870112 00870114 00870116 00870118 00870120 00870122 00870124 00870126 00870128 00870130 00870132 00870134 00870136 00870138 00870140 00870142 00870144 00870146 00870148 00870150 00870152 00870154 00870156 00870158 00870160 00870162 00870164 00870166 00870168 00870170 00870172 00870174 00870176 00870178 00870180 00870182 00870184 00870186 00870188 00870190 00870192 00870194 00870196 00870198 00870200 00870202 00870204 00870206 00870208 00870210 00870212 00870214 00870216 00870218 00870220 00870222 00870224 00870226 00870228 00870230 00870232 00870234 00870236 00870238 00870240 00870242 00870244 00870246 00870248 00870250 00870252 00870254 00870256 00870258 00870260 00870262 00870264 00870266 00870268 00870270 00870272 00870274 00870276 00870278 00870280 00870282 00870284 00870286 00870288 00870290 00870292 00870294 00870296 00870298 00870300 00870302 00870304 00870306 00870308 00870310 00870312 00870314 00870316 00870318 00870320 00870322 00870324 00870326 00870328 00870330 00870332 00870334 00870336 00870338 00870340 00870342 00870344 00870346 00870348 00870350 00870352 00870354 00870356 00870358 00870360 00870362 00870364 00870366 00870368 00870370 00870372 00870374 00870376 00870378 00870380 00870382 00870384 00870386 00870388 00870390 00870392 00870394 00870396 00870398 00870400 00870402 00870404 00870406 00870408 00870410 00870412 00870414 00870416 00870418 00870420 00870422 00870424 00870426 00870428 00870430 00870432 00870434 00870436 00870438 00870440 00870442 00870444 00870446 00870448 00870450 00870452 00870454 00870456 00870458 00870460 00870462 00870464 00870466 00870468 00870470 00870472 00870474 00870476 00870478 00870480 00870482 00870484 00870486 00870488 00870490 00870492 00870494 00870496 00870498 00870500 00870502 00870504 00870506 00870508 00870510 00870512 00870514 00870516 00870518 00870520 00870522 00870524 00870526 00870528 00870530 00870532 00870534 00870536 00870538 00870540 00870542 00870544 00870546 00870548 00870550 00870552 00870554 00870556 00870558 00870560 00870562 00870564 00870566 00870568 00870570 00870572 00870574 00870576 00870578 00870580 00870582 00870584 00870586 00870588 00870590 00870592 00870594 00870596 00870598 00870600 00870602 00870604 00870606 00870608 00870610 00870612 00870614 00870616 00870618 00870620 00870622 00870624 00870626 00870628 00870630 00870632 00870634 00870636 00870638 00870640 00870642 00870644 00870646 00870648 00870650 00870652 00870654 00870656 00870658 00870660 00870662 00870664 00870666 00870668 00870670 00870672 00870674 00870676 00870678 00870680 00870682 00870684 00870686 00870688 00870690 00870692 00870694 00870696 00870698 00870700 00870702 00870704 00870706 00870708 00870710 00870712 00870714 00870716 00870718 00870720 00870722 00870724 00870726 00870728 00870730 00870732 00870734 00870736 00870738 00870740 00870742 00870744 00870746 00870748 00870750 00870752 00870754 00870756 00870758 00870760 00870762 00870764 00870766 00870768 00870770 00870772 00870774 00870776 00870778 00870780 00870782 00870784 00870786 00870788 00870790 00870792 00870794 00870796 00870798 00870800 00870802 00870804 00870806 00870808 00870810 00870812 00870814 00870816 00870818 00870820 00870822 00870824 00870826 00870828 00870830 00870832 00870834 00870836 00870838 00870840 00870842 00870844 00870846 00870848 00870850 00870852 00870854 00870856 00870858 00870860 00870862 00870864 00870866 00870868 00870870 00870872 00870874 00870876 00870878 00870880 00870882 00870884 00870886 00870888 00870890 00870892 00870894 00870896 00870898 00870900 00870902 00870904 00870906 00870908 00870910 00870912 00870914 00870916 00870918 00870920 00870922 00870924 00870926 00870928 00870930 00870932 00870934 00870936 00870938 00870940 00870942 00870944 00870946 00870948 00870950 00870952 00870954 00870956 00870958 00870960 00870962 00870964 00870966 00870968 00870970 00870972 00870974 00870976 00870978 00870980 00870982 00870984 00870986 00870988 00870990 00870992 00870994 00870996 00870998 00871000 00871002 00871004 00871006 00871008 00871010 00871012 00871014 00871016 00871018 00871020 00871022 00871024 00871026 00871028 00871030 00871032 00871034

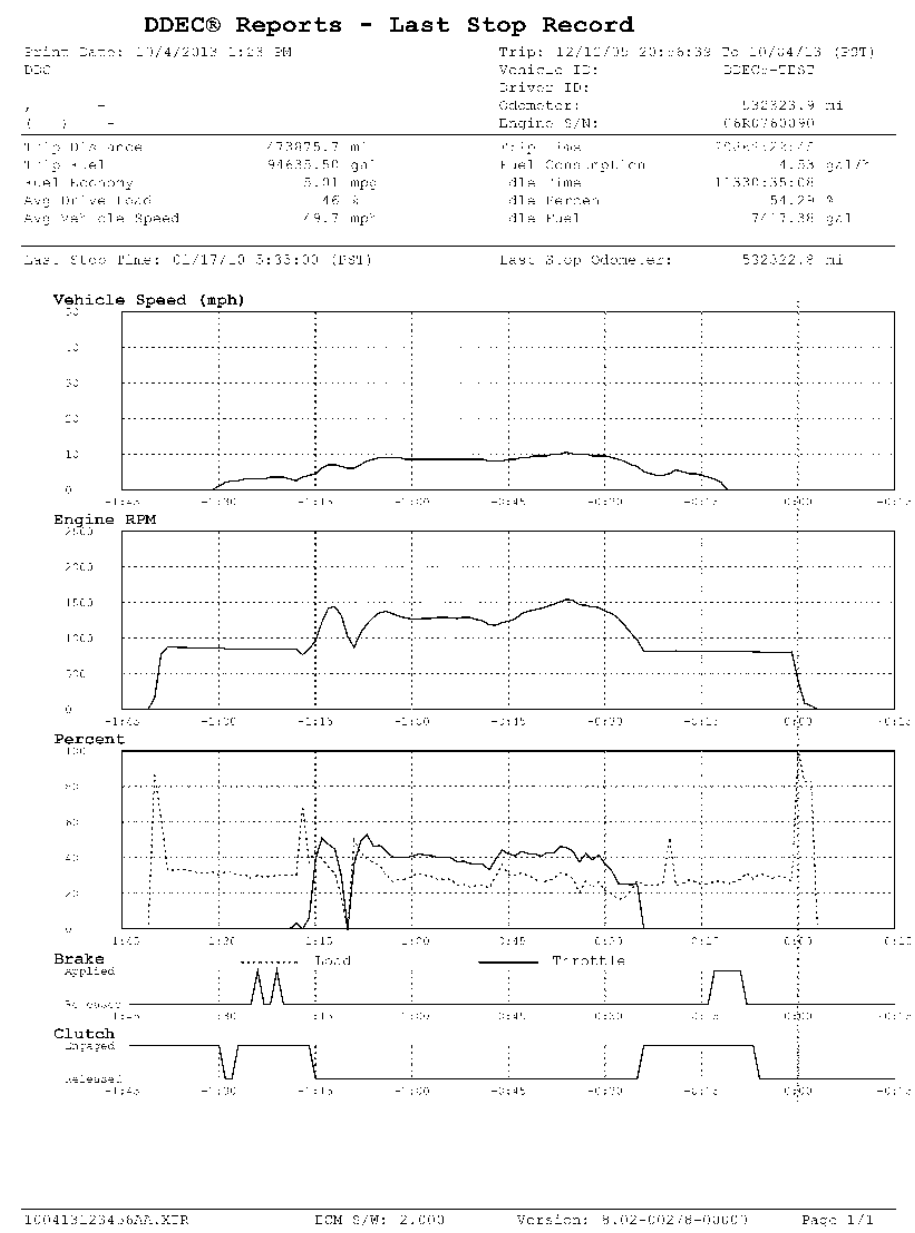
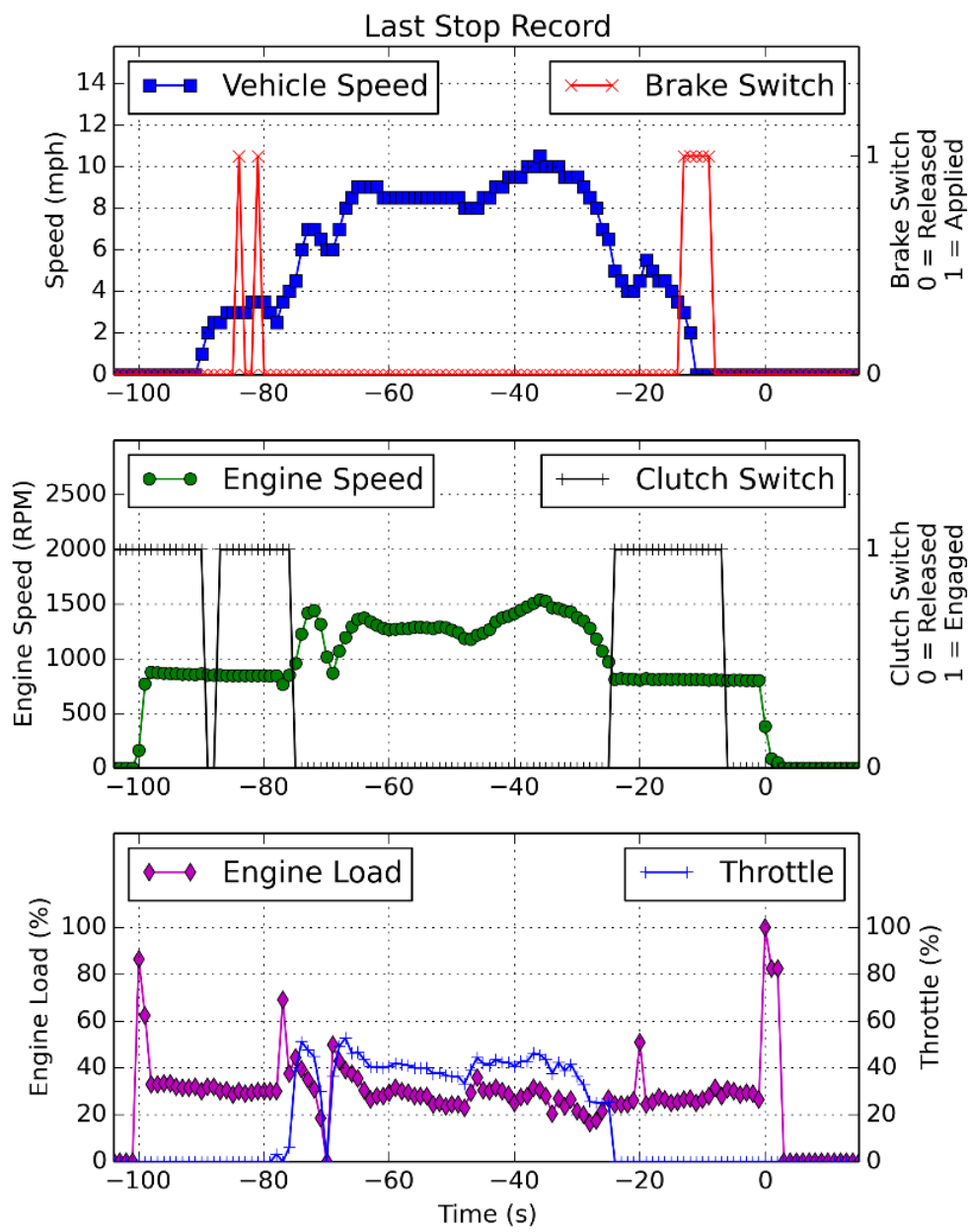
Hard Brake 1 Comparison



Hard Brake 2 Comparison



Last Stop Comparison



Daily Engine Usage

DDEC® Reports - Daily Engine Usage

Print Date: 8/21/2013 11:08 AM

Date Range: 01/18/07 To 01/07/00 (EST)

University of Tulsa

800 S. Tucker Dr

Tulsa, OK 74104

(918) 631-3056

Vehicle ID:

TIB DDEC4

Driver ID:

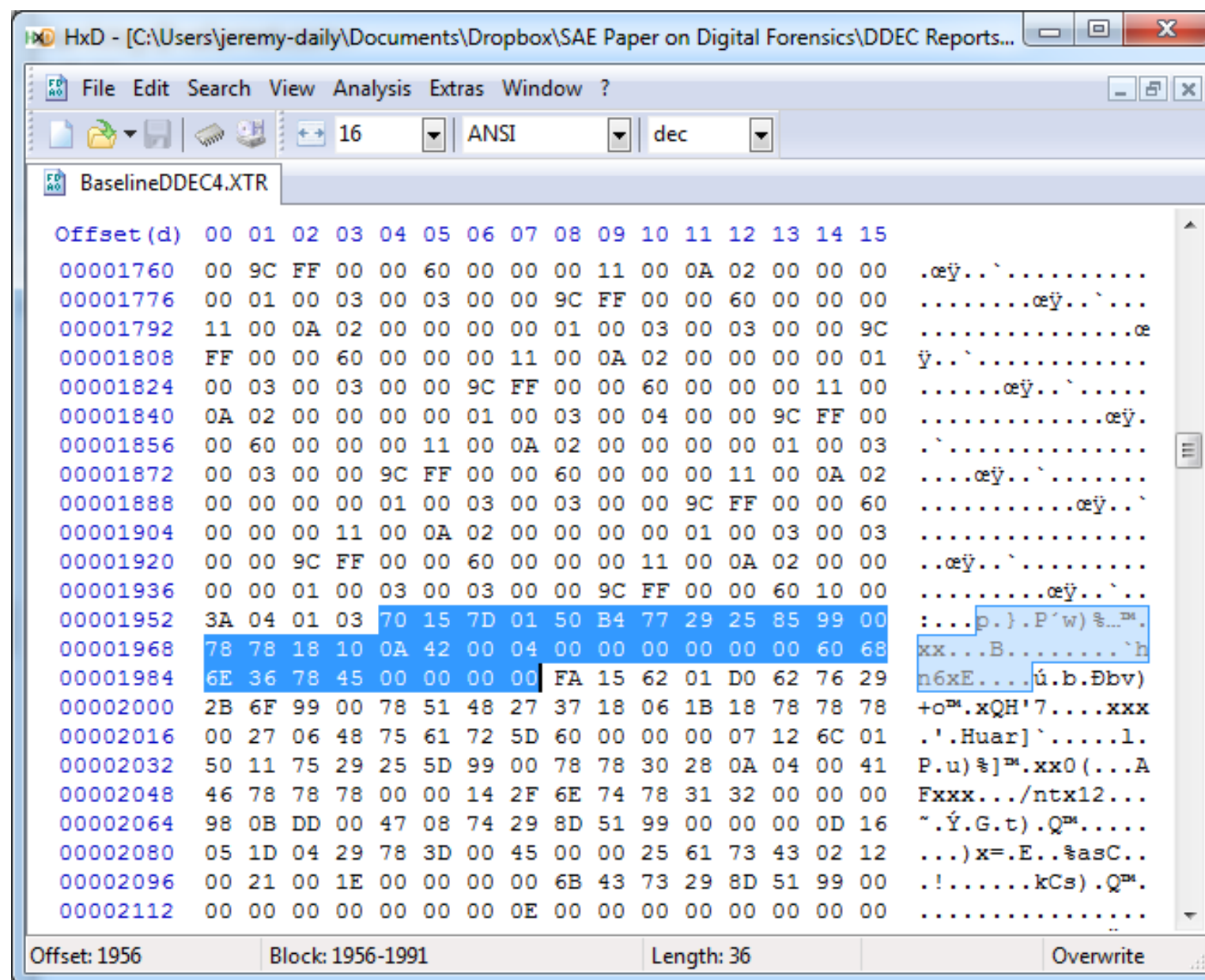
Engine S/N:

06R0499534

Date:	1/18/2007
Start Time:	00:00:00 EST
Odometer:	1006109.00 mi
Distance:	548.80 mi
Fuel:	95.25 gal
Fuel Economy:	5.76 mpg
Average Speed:	59.54 mph

Total (hh:mm)	09:13	06:00	08:47
Hour (EST)	Drive (min)	Idle (min)	Off (min)
00:00-02:00	0	120	0
02:00-04:00	0	120	0
04:00-06:00	96	24	0
06:00-08:00	104	16	0
08:00-10:00	110	10	0
10:00-12:00	54	66	0
12:00-14:00	120	0	0
14:00-16:00	69	4	47
16:00-18:00	0	0	120
18:00-20:00	0	0	120
20:00-22:00	0	0	120
22:00-24:00	0	0	120

Daily Engine Usage Log Data - .XTR file



The screenshot shows the HxD hex editor interface. The title bar indicates the file path: C:\Users\jeremy-daily\Documents\Dropbox\SAE Paper on Digital Forensics\DDEC Reports... The menu bar includes File, Edit, Search, View, Analysis, Extras, and Window. The toolbar shows icons for file operations and a status bar at the bottom displays 'Offset: 1956', 'Block: 1956-1991', 'Length: 36', and 'Overwrite'. The main display area shows a hex dump of the file 'BaselineDDEC4.XTR'. The first column lists offsets from 00001760 to 00002112 in increments of 16. The subsequent columns show hex values in groups of 16. The rightmost column shows the corresponding ASCII text. A portion of the data is highlighted in blue, corresponding to the selected block.

Offset (d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	ASCII
00001760	00	9C	FF	00	00	60	00	00	00	11	00	0A	02	00	00	00	.œÿ...`.....
00001776	00	01	00	03	00	03	00	00	9C	FF	00	00	60	00	00	00œÿ...`...
00001792	11	00	0A	02	00	00	00	00	01	00	03	00	03	00	00	9Cœ
00001808	FF	00	00	60	00	00	00	11	00	0A	02	00	00	00	00	01	ÿ...`.....
00001824	00	03	00	03	00	00	9C	FF	00	00	60	00	00	00	11	00œÿ...`.....
00001840	0A	02	00	00	00	00	01	00	03	00	04	00	00	9C	FF	00œÿ.
00001856	00	60	00	00	00	11	00	0A	02	00	00	00	00	01	00	03	.`.....
00001872	00	03	00	00	9C	FF	00	00	60	00	00	00	11	00	0A	02œÿ...`.....
00001888	00	00	00	00	01	00	03	00	03	00	00	9C	FF	00	00	60œÿ...`
00001904	00	00	00	11	00	0A	02	00	00	00	00	01	00	03	00	03
00001920	00	00	9C	FF	00	00	60	00	00	00	11	00	0A	02	00	00	..œÿ...`.....
00001936	00	00	01	00	03	00	03	00	00	9C	FF	00	00	60	10	00œÿ...`..
00001952	3A	04	01	03	70	15	7D	01	50	B4	77	29	25	85	99	00p.).P'w)§...™.
00001968	78	78	18	10	0A	42	00	04	00	00	00	00	00	00	60	68	xx...B.....`h
00001984	6E	36	78	45	00	00	00	00	FA	15	62	01	D0	62	76	29	n6xE....ú.b.Đbv)
00002000	2B	6F	99	00	78	51	48	27	37	18	06	1B	18	78	78	78	+o™.xQH'7....xxx
00002016	00	27	06	48	75	61	72	5D	60	00	00	00	07	12	6C	01	.'.Huar]`.....l.
00002032	50	11	75	29	25	5D	99	00	78	78	30	28	0A	04	00	41	P.u)§]™.xx0 (...A
00002048	46	78	78	78	00	00	14	2F	6E	74	78	31	32	00	00	00	Fxxx.../ntx12...
00002064	98	0B	DD	00	47	08	74	29	8D	51	99	00	00	00	0D	16	~.Ý.G.t).Q™.....
00002080	05	1D	04	29	78	3D	00	45	00	00	25	61	73	43	02	12	...)x=.E..§asC..
00002096	00	21	00	1E	00	00	00	00	6B	43	73	29	8D	51	99	00	.!.....kCs).Q™.
00002112	00	00	00	00	00	00	00	0E	00	00	00	00	00	00	00	00

Determining Data Meaning in the Daily Engine Usage Log

Interpreted Data

Bytes Sequence	Hex Value (s)	Decimal	LSB Value	Meaning	Value
0-1	70 15	5488	0.1 mile	Distance	548.8 miles
2-3	7D 01	381	0.25 gal	Fuel	95.25 gallons
4-7	50 B4 77 29	695710800	1 sec from epoch	Start Time	17 Jan 2007 at 23:00:00 CST
8-11	25 85 99 00	10061093	0.1 mile	Odometer	1006109.3 miles
12-23	78 78 18 10 0A 42 00 04 00 00 00 00	120 120 24 16 10 66 0 4 0 0 0 0	1 Minute	Idle Time	Same as Decimal
24-35	00 00 60 68 6E 36 78 45 00 00 00 00	0 0 96 104 54 120 69 0 0 0 0	1 Minute	Drive Time	Same as Decimal

All other data are calculated
Interestingly, the .XTR file contains minutes, but the chip memory contains seconds.

Chip Memory Contents

XTR file has 36 Bytes for 1 day in the Daily Engine Usage Log.

However... The memory record containing the Daily Engine Usage data is contained in a circular 30-day buffer with each day holding 66 bytes.

This was determined by locating the odometer readings since the MSB's were the same. There were 66 bytes from one 4-byte odometer reading to another.

Data Description	Unit	Location and sequence	Word Size (LSB last)	LSB Value	Example
Start Time Stamp	Seconds	1, 0, 3, 2	U32	1	Figure 16
Odometer	Miles	5, 4, 7, 6	U32	1/640	Figure 17
Distance Traveled	Miles	9, 8, 11, 10	U32	1/640	Figure 18
Fuel Used	Gallons	12, 13	U16	0.125	Figure 19

Daily Engine Usage Time

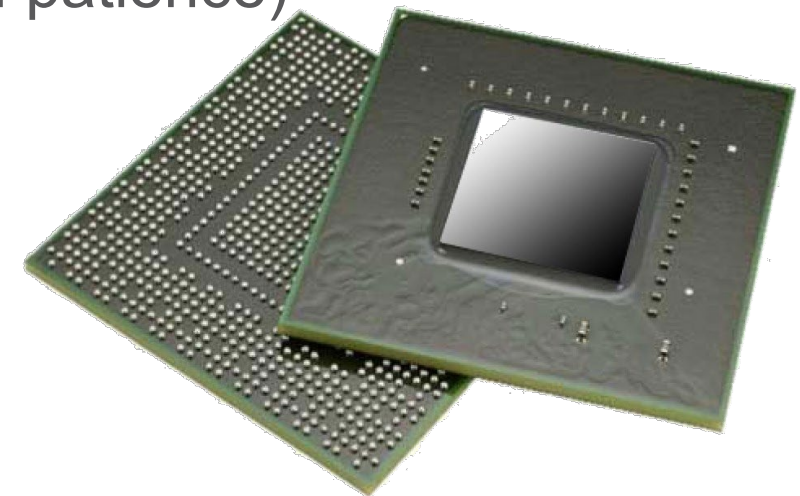
- XTR file = 24 bytes
- Memory Chips = 48 bytes, so there twice the bytes that are in memory but not transmitted on the network.
- XTR file has minutes coded as single bytes (0-255)
- Memory stores times in seconds as 2 bytes (16 bit) (0-65536)
- Only Drive time and Idle time in each 2-hour block are recorded in memory.
- Drive + Idle seconds in memory contents did not always sum to 7200 seconds (2 hours)

Decoded Daily Engine Usage Log

Start Date	Start Time	Odometer	Distance	Fuel	Total Daily Time		00:00-02:00		02:00-04:00		04:00-06:00		06:00-08:00		...
Central Standard Time		Miles	Miles	Gallons	Idle (HH:MM)	Drive (HH:MM)	Idle	Drive	Idle	Drive	Idle	Drive	Idle	Drive	
Thu, 07 Jan 2010	02:00:00AM	530196.8	346.5	76.750	15:23	08:04	82:33	26:49	65:43	54:17	20:38	99:22	55:49	41:00	
Fri, 08 Jan 2010	02:00:00AM	530543.3	470.0	111.625	13:60	09:58	120:00	00:00	108:47	11:12	00:00	120:00	05:12	114:48	
Sat, 09 Jan 2010	02:00:00AM	531013.3	506.1	111.750	13:57	09:43	120:00	00:00	120:00	00:00	49:13	49:57	03:28	116:33	

Issues

- Broken ECUs usually lose power before the events have a chance to write.
- Hard Brake and Last Stop data are from the previous events (i.e. not interesting).
- The process of removing the chip is destructive.
- Reinstalling the chip requires special equipment (and patience)
- Ball Grid Array (BGA) chips are particularly challenging.



<https://www.forentec.ch/weitere-services/mobile-forensics-training/teeltech-bga-chip-off-forensic/>

Sometimes there are
serious issues...



Missing Data??



Can we read memory in place?

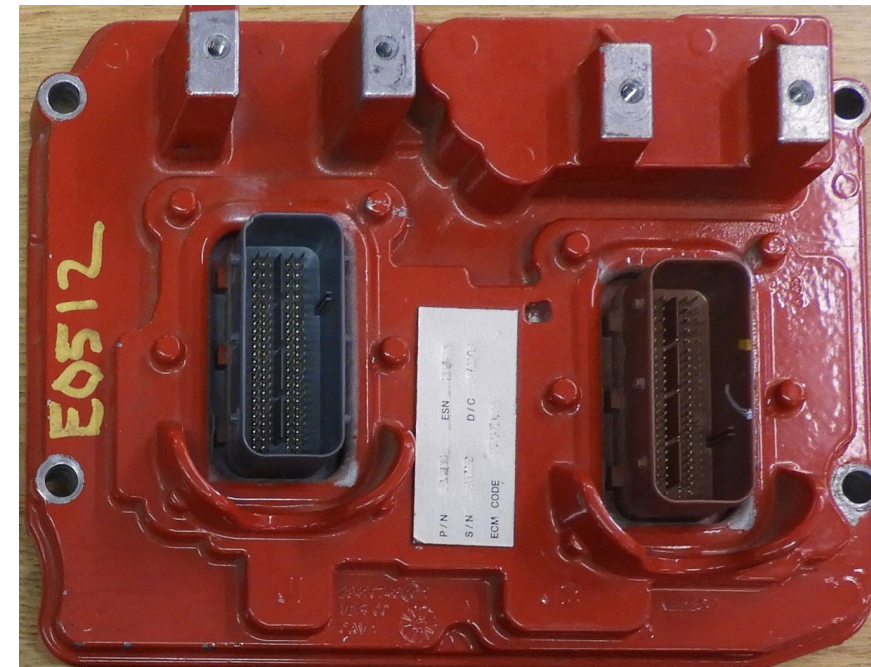
The chip removal method is challenging.

Case Study: Cummins

Cummins CM870
(MPC5xx)



Cummins CM2350
(MPC55xx-57xx)

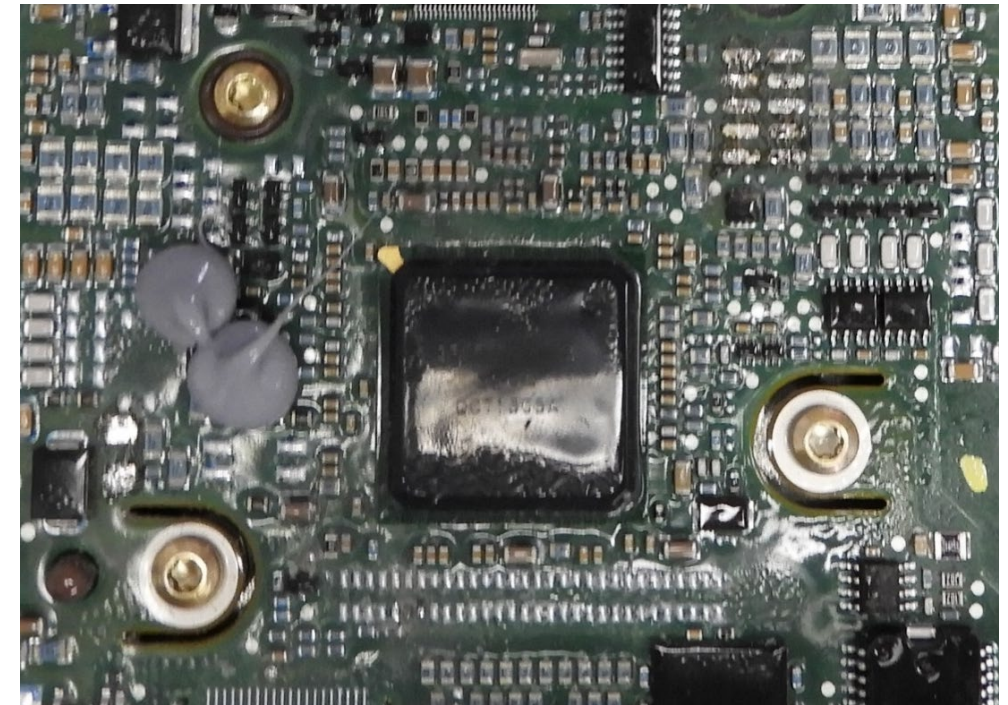


Case Study: Cummins

Cummins CM870
(MPC5xx)

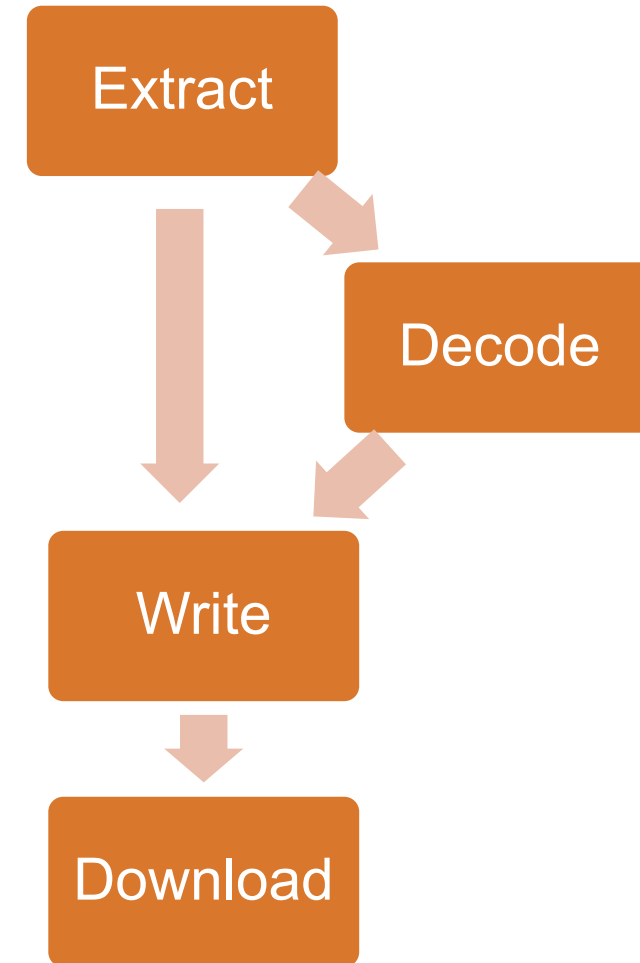


Cummins CM2350
(MPC5674F)



Goals and Objectives

- Safely extract binary data from the broken ECU
- Decode the extracted data to recover
 - Sudden Deceleration Records
 - Data Plate Information
 - Fault Codes
 - Parameters and Settings
- Write the extracted binary to a working ECU
- Download the data using diagnostic or forensic computer programs



Data Extraction via the JTAG Port

- Use the Joint Test Action Group (JTAG) specified programming port for the microprocessor on the ECUs printed circuit board.
- Case study used the following tools:

AlienTech K-TAG Master kit



PEmicro CYCLONE FX Programmer



Using the K-TAG Tool

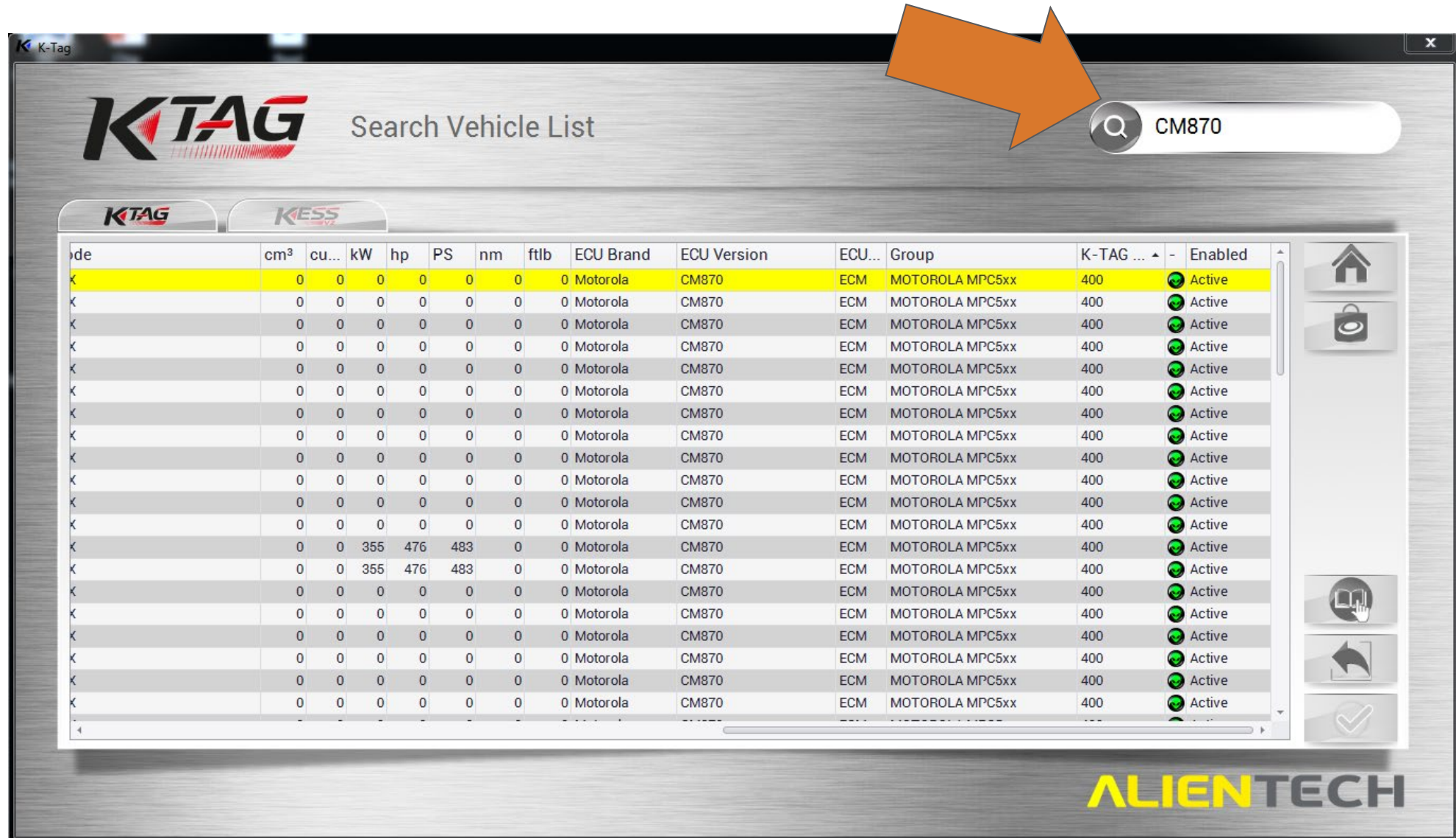
Example for the CM870



K-TAG Software Startup

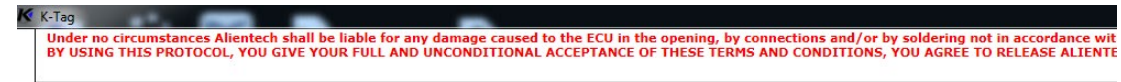


Search for ECM



Locate the JTAG Port

- After choosing the correct ECU, click on the bookmark icon for wiring instruction



Instructions

1. Remove the ECU from the vehicle;
2. Open the ECU, being careful not to damage the parts inside;
3. **Reconnect the ECU to the vehicle and start the engine, in order to make sure the ECU is still in working order and has not been damaged in**
4. Remove again the ECU from the vehicle;
5. **Connect to the ECU:**

The programming pads are shown in red in the picture.

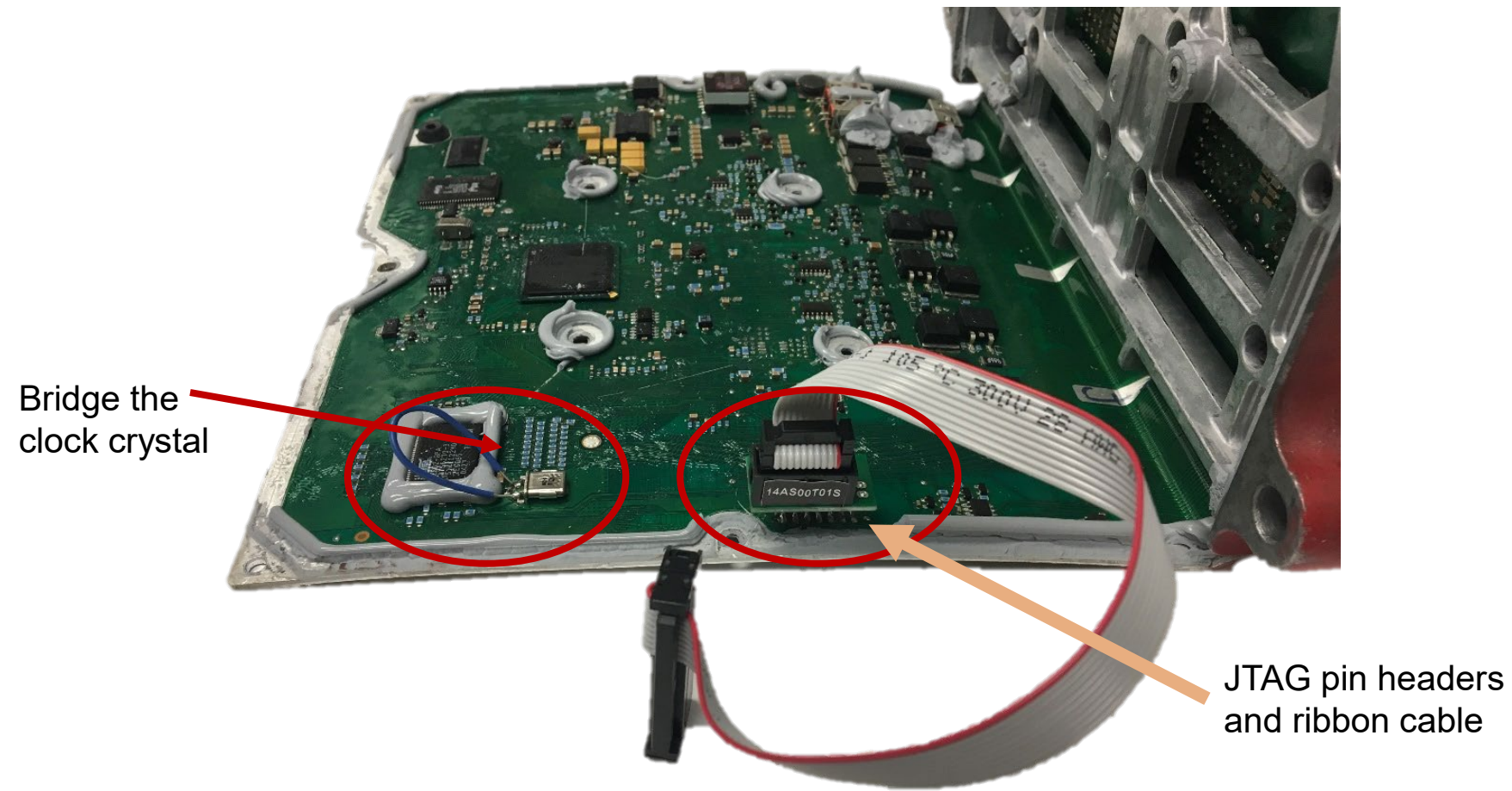
Note: Open the ECU cover on the side without connector.



6. **Always** make a full backup of the ECU;
7. Proceed with **reading/writing**.

JTAG Port Connection

- Follow the instruction on the software, solder the port and attach the ribbon.



Connect Power

- Attach the D-sub cable to the ECU connector
- Power
- Ignition

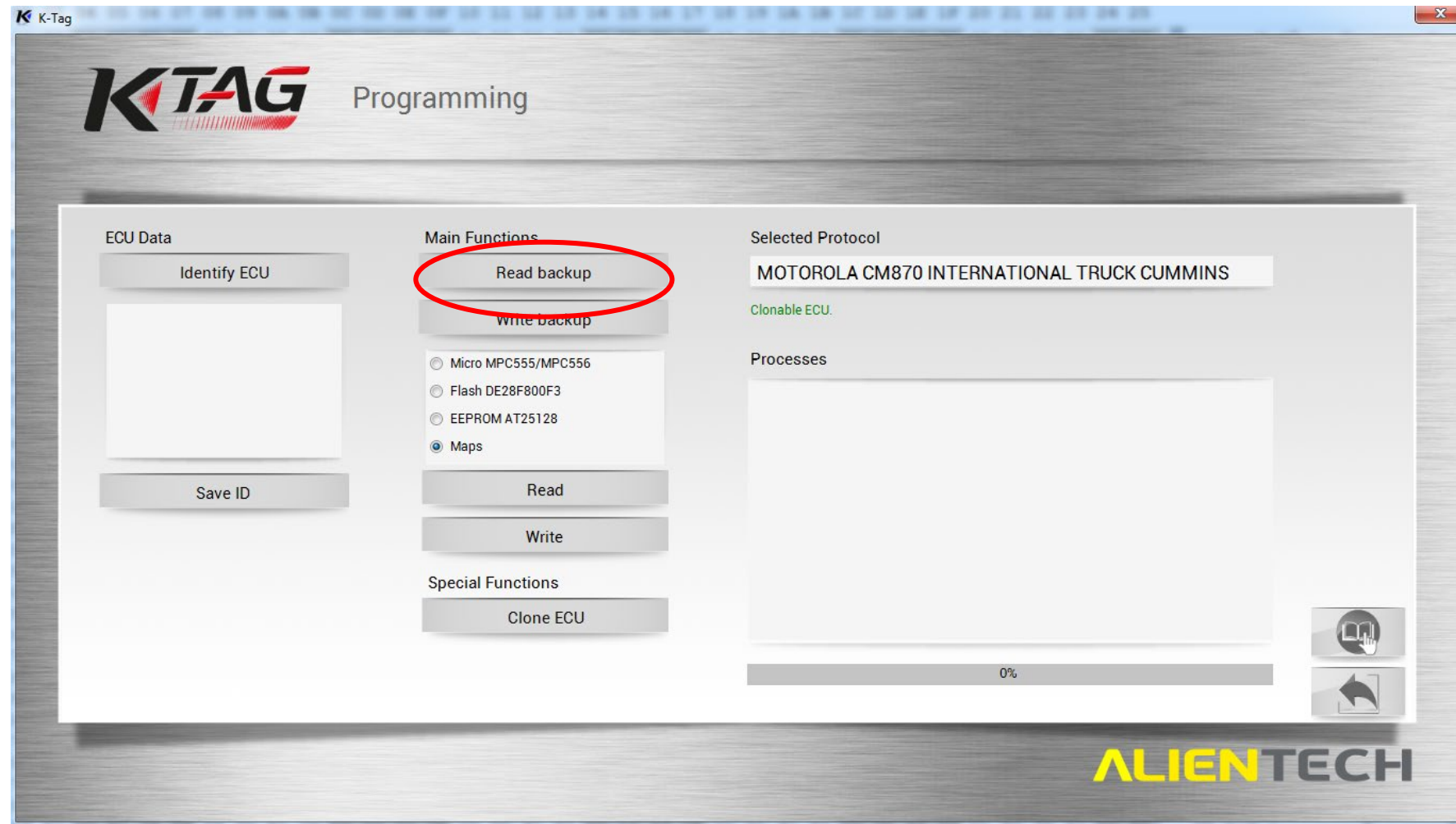


PC Connection Setup

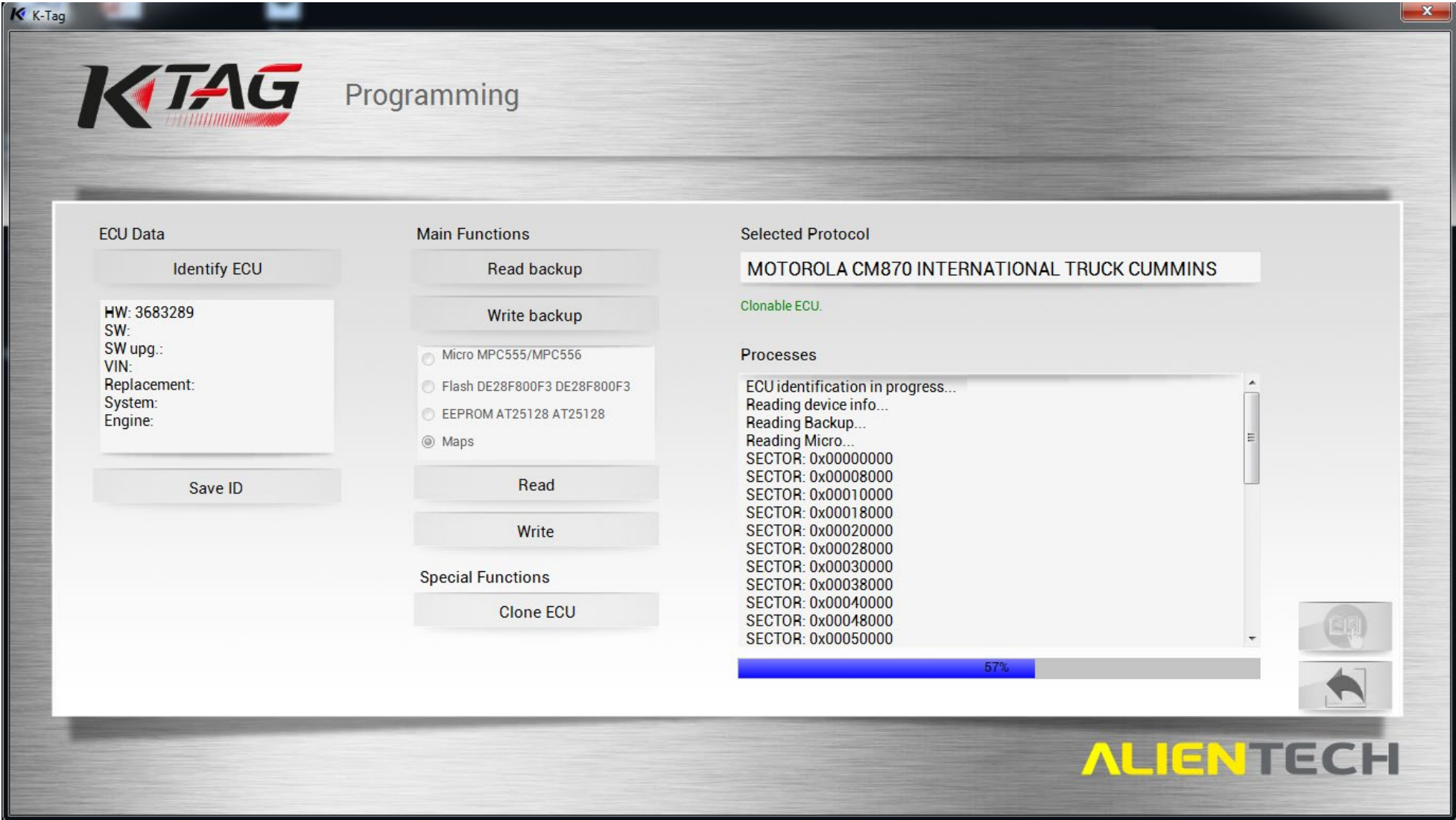
- Connect the KTAG to the ECU and the computer



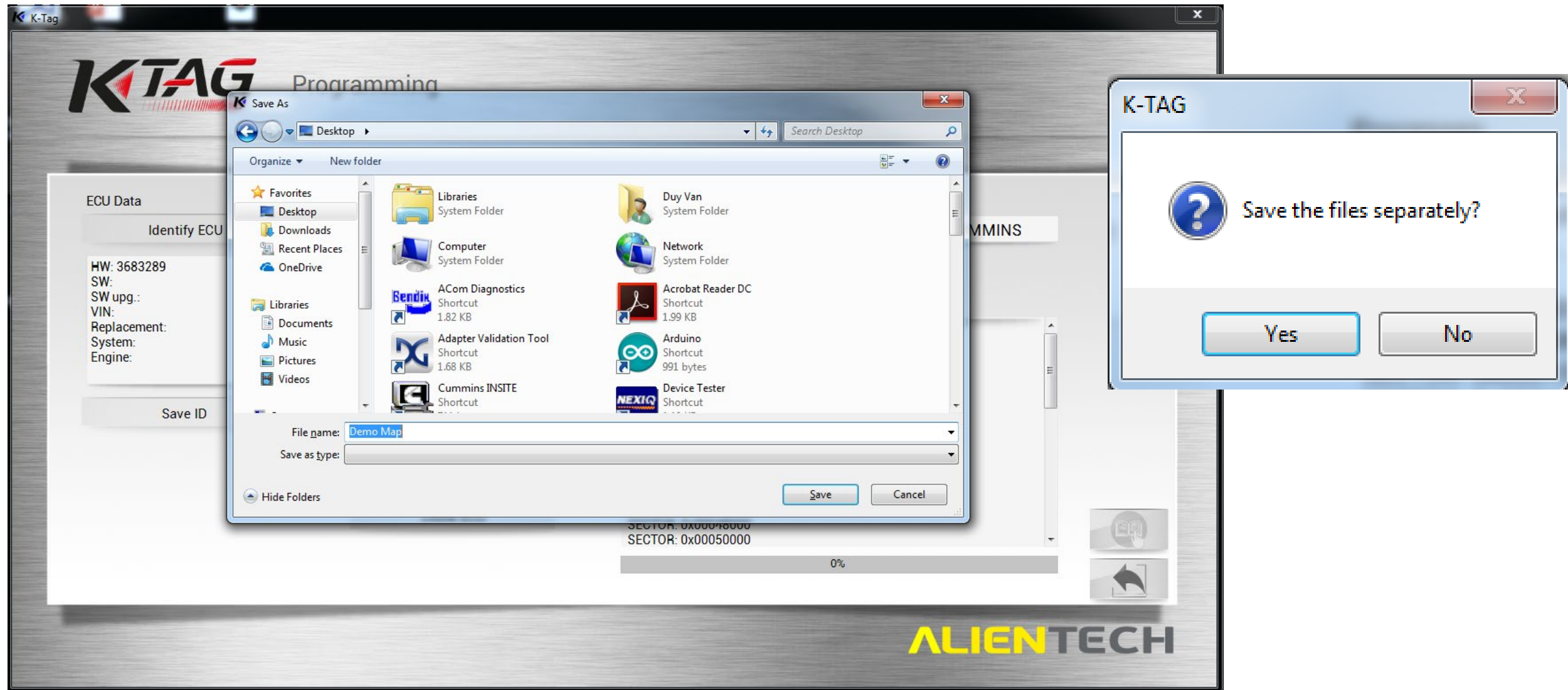
Retrieving Data



Retrieving Data



Save the Binary Data



Binary Result in Hex Editor

Demo Map.MPC - Hexinator

File Edit View Grammar Script Window Help

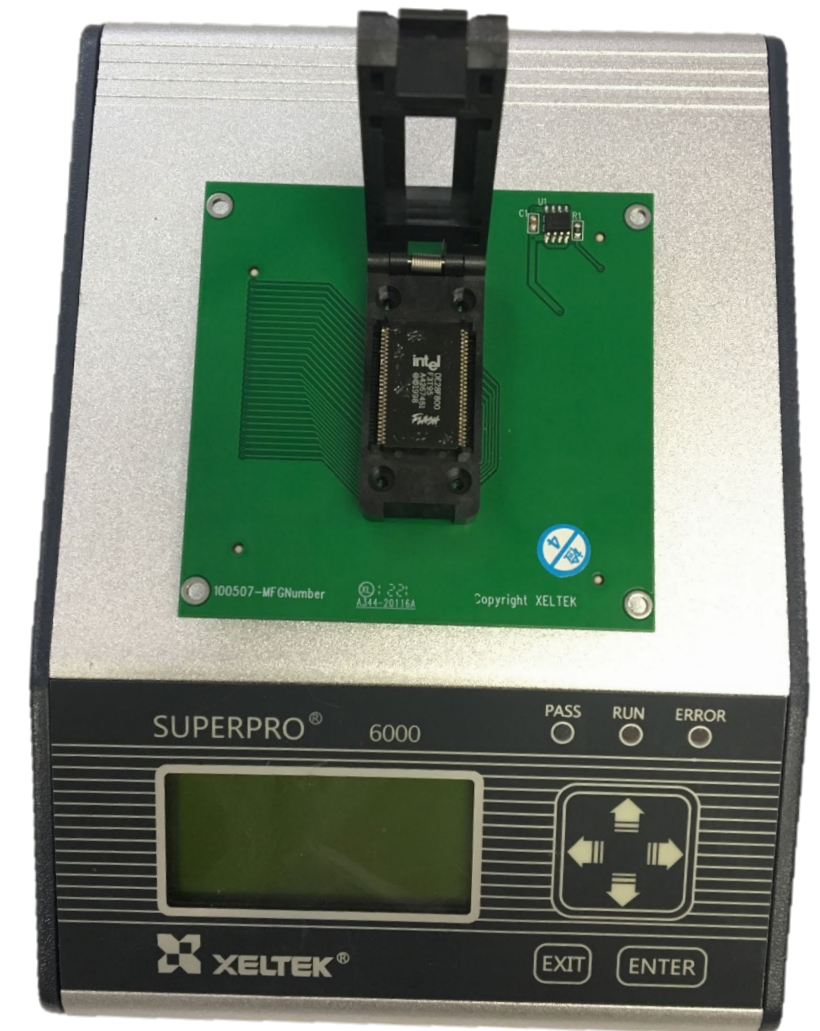
Go To Position: ISO_8859-1:1987 Encoding: <none> Grammar: <none> Parse: <none> Results Script: Process Results

	00	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	21	22	23	24	25	
0x00000	48	00	04	82	00	00	00	00	48	00	28	D2	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	
0x00026	00	00	48	00	02	DA	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	48	00	03	AE		
0x0004C	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	48	00		
0x00072	04	82	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00			
0x00098	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	48	00	04	82	00			
0x000BE	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	48	00	04			
0x000E4	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	00	48	00	04	82	00	00	00	00	48	00	28	D2	00	00	28	D0	00		
0x0010A	00	00	31	32	31	38	30	32	04	06	00	01	0C	08	00	00	12	01	10	01	FF	FF	FF	40	FE	0A	01	00	00	01	01	02	00	01	09	02	2E	00	
0x00130	01	01	04	C0	00	00	09	04	00	00	04	FF	FF	FF	05	00	07	05	03	02	40	00	00	00	07	05	84	02	40	00	00	00	07	05	07	02	40	00	
0x00156	00	00	07	05	88	02	40	00	00	00	09	04	43	75	6D	6D	69	6E	73	20	49	6E	63	2E	00	00	43	75	6D	6D	69	6E	73	20	49	6E	63	2E	
0x0017C	20	45	6E	67	69	6E	65	20	43	6F	6E	74	72	6F	6C	20	4D	6F	64	75	6C	65	00	00	53	65	6C	66	2D	70	6F	77	65	72	65	64	20	77	
0x001A2	69	74	68	20	6F	6E	65	20	49	6E	74	65	72	66	61	63	65	00	42	75	6C	6B	20	63	6F	6E	6E	65	63	74	69	6F	6E	20	66	6F	72	20	
0x001C8	61	70	70	6C	69	63	61	74	69	6F	6E	73	00	00	FF	FF	94	21	FF	D8	7C	08	02	A6	90	01	00	2C	3C	C0	00	B1	38	C6	97	A3	80	E6	
0x001EE	00	00	81	46	00	08	7C	87	50	50	2C	04	00	00	40	81	00	0C	38	A0	FF	FE	48	00	00	08	38	A0	00	FE	7C	A4	2A	14	2C	05	00	02	
0x00214	40	81	00	B4	90	E1	00	0C	90	E1	00	08	89	81	00	0B	39	8C	00	01	99	81	00	0B	2C	03	00	00	40	82	00	0C	38	E0	00	64	48	00	
0x0023A	00	3C	2C	03	00	01	40	82	00	0C	38	E0	00	74	48	00	00	10	38	E0	00	75	2C	03	00	12	40	80	00	08	48	00	00	14	3D	80	00	01	
0x00260	39	8C	8D	D0	7D	63	1A	14	7C	6C	5A	2E	3D	80	00	B1	B0	6C	95	05	81	81	00	08	39	60	00	06	99	6C	00	00	89	41	00	0B	39	4A	
0x00286	00	01	99	41	00	0B	81	81	00	08	98	EC	00	00	89	61	00	0B	39	6B	00	01	99	61	00	0B	81	41	00	0C	39	80	00	02	99	8A	00	00	
0x002AC	81	21	00	0C	91	26	00	08	80	61	00	08	90	66	00	00	39	40	00	00	99	43	00	00	48	00	13	7D	80	01	00	2C	7C	08	03	A6	38	21	
0x002D2	00	28	4E	80	00	20	94	21	FF	B0	90	01	00	08	7C	1A	02	A6	90	01	00	0C	7C	1B	02	A6	90	01	00	10	7C	09	02	A6	90	01	00	14	
0x002F8	7C	01	02	A6	90	01	00	18	7C	00	00	26	90	01	00	1C	7C	08	02	A6	90	01	00	20	90	61	00	28	90	81	00	2C	90	A1	00	30	90	C1	
0x0031E	00	34	90	E1	00	38	91	01	00	3C	91	21	00	40	91	41	00	44	91	61	00	48	91	81	00	4C	3D	80	00	01	81	8C	00	5A	7D	88	03	A6	
0x00344	4E	80	00	21	80	61	00	28	80	81	00	2C	80	A1	00	30	80	C1	00	34	80	E1	00	38	81	01	00	3C	81	21	00	40	81	41	00	44	81	61	
0x0036A	00	48	81	81	00	4C	80	01	00	20	7C	08	03	A6	80	01	00	1C	7C	0F	F1	20	80	01	00	18	7C	01	03	A6	80	01	00	14	7C	09	03	A6	
0x00390	80	01	00	10	7C	1B	03	A6	80	01	00	0C	7C	1A	03	A6	80	01	00	08	38	21	00	50	4C	00	00	64	94	21	FF	B0	90	01	00	08	7C	1A	
0x003B6	02	A6	90	01	00	0C	7C	1B	02	A6	90	01	00	10	7C	09	02	A6	90	01	00	14	7C	01	02	A6	90	01	00	18	7C	00	00	26	90	01	00	1C	
0x003DC	7C	08	02	A6	90	01	00	20	90	61	00	28	90	81	00	2C	90	A1	00	30	90	C1	00	34	90	E1	00	38	91	01	00	3C	91	21	00	40	91	41	
0x00402	00	44	91	61	00	48	91	81	00	4C	3D	80	00	01	81	8C	00	5E	7D	88	03	A6	4E	80	00	21	80	61	00	28	80	81	00	2C	80	A1	00	30	
0x00428	80	C1	00	34	80	E1	00	38	81	01	00	3C	81	21	00	40	81	41	00	44	81	61	00	48	81	81	00	4C	80	01	00	20	7C	08	03	A6	80	01	
0x0044E	00	1C	7C	0F	F1	20	80	01	00	18	7C	01	03	A6	80	01	00	14	7C	09	03	A6	80	01	00	10	7C	1B	03	A6	80	01	00	0C	7C	1A	03	A6	
0x00474	80	01	00	08	38	21	00	50	4C	00	00	64	94	21	FF	B0	90	01	00	08	7C	1A	02	A6	90	01	00	0C	7C	1B	02	A6	90	01	00	10	7C	09	
0x0049A	02	A6	90	01	00	14	7C	01	02	A6	90	01	00	18	7C	00	00	26	90	01	00	10	7C	01	02	A6	90	01	00	1B	02	90	61	00	28	90	81	00	2C
0x004C0	90	A1	00	30	90	C1	00	34	90	E1	00	38	91	01	00	3C	91	21	00	40	91	41	00	44	91	61	00	48	91	81	00	4C	3D	80	00	01	81	8C	
0x004E6	00	62	7D	88	03	A6	4E	80	00	21	80	61	00	28	80	81	00	2C	80	A1	00	30	80	C1	00	34	80	E1	00	38	81	01	00	3C	81	21	00	40	
0x0050C	81	41	00	44	81	61	00	48	81	81	00	4C	80	01	00	20	7C	08	03	A6	80	01	00	1C	7C	0F	F1	20	80	01	00	18	7C	01	03	A6	80	01	
0x00532	00	14	7C	09	03	A6	80	01	00	10	7C	1B	03	A6	80	01	00	0C	7C	1A	03	A6	80	01	00	08	38	21	00	50	4C	00	00	64	7C	04	18	40	
0x00558	41	80	00	0C	7C	63	20	50	48	00	00	0C	7C	64	18	50	20	63	00	00	4E	80	00	20	94	21	FF	E8	7C	08	02	A6	BF	A1	00	0C	90	01	
0x0057E	00	1C	3F	E0	00	B1	3B	FF	8F	7C	81	7F	00	00	2C	0B	00	00	41	82	00	10	2C	0B	00	01	41	82	00	38	48	00	01	60	3D	80	00	30	
0x005A4	A1	8C	61	00	55	8C	06	B4	2C	0C	00	00	40	82	00	10	39	80	00	01	91	9F	00	00	48	00	01	40	3D	80	00	B1	39	60	00	00	B1	6C	

Start	End	Length	Content
0x574	0x574	1	7C

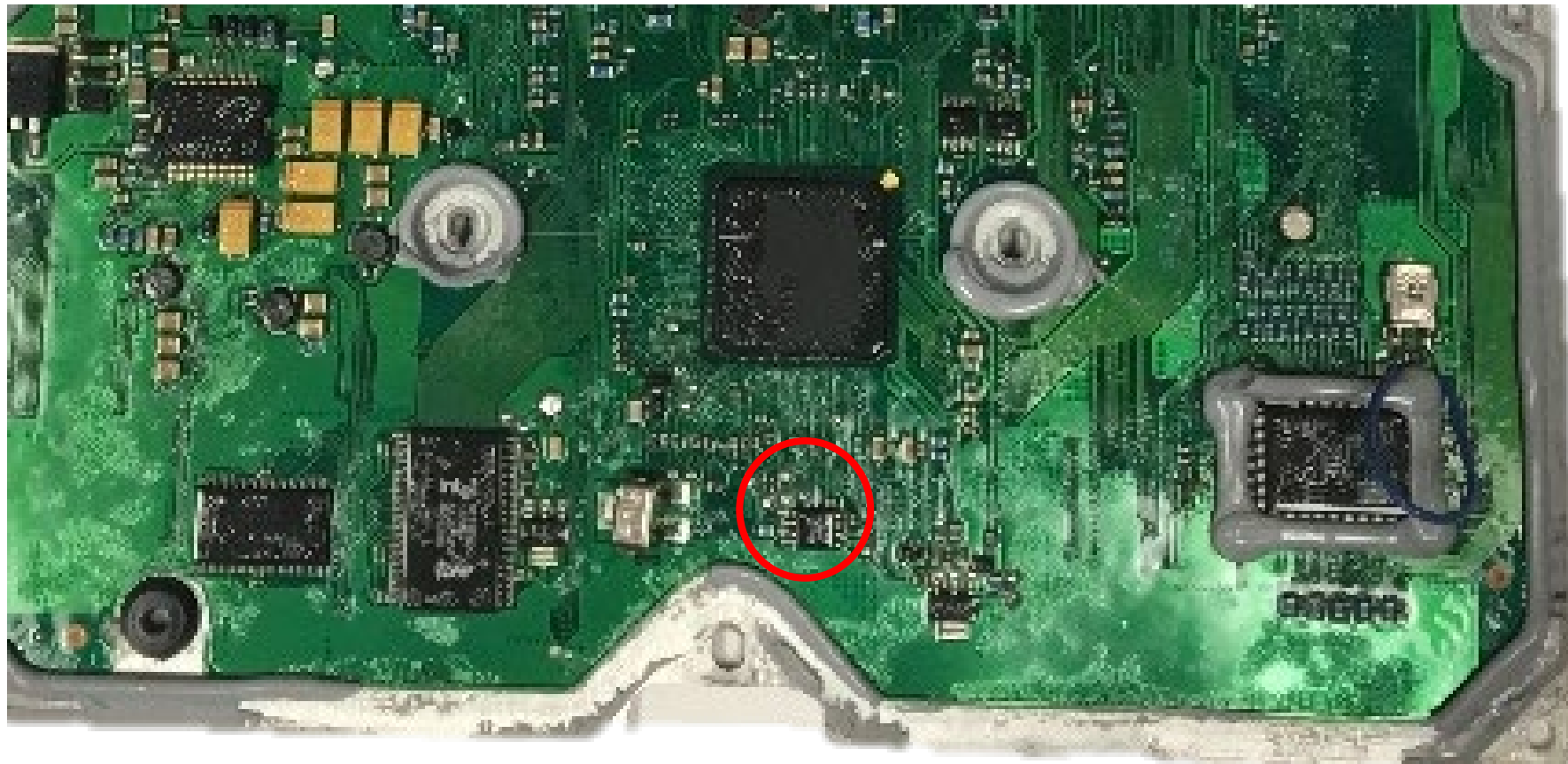
Chip Level Access for Flash

- Flash chip, can be retrieved using individual chip reader



Chip Level Access: EEPROM

- For CM870, EEPROM carries dataplate information via ASCII



Dataplate Attribution Data

- Closer look at PowerSpec and EEPROM (for CM870)

Engine Dataplate Report			
Engine Type	ISX 02	Ecm Code	AB10402.22
Engine Serial Number	79076145	Software Phase	6.5.4.2
Unit Number	25175	Extraction Date	04-02-2018 05:48:00

ECM Information

Module Name	CM870
Ecm Code	AB10402.22
Software Phase	6.5.4.2
ECM Serial Number	23052876
ECM Part Number	3683289

Engine Information

Engine Model	ISX 02
Engine Build Date	N/A
Engine Serial Number	79076145
Do Option	1325
SC Option	11145

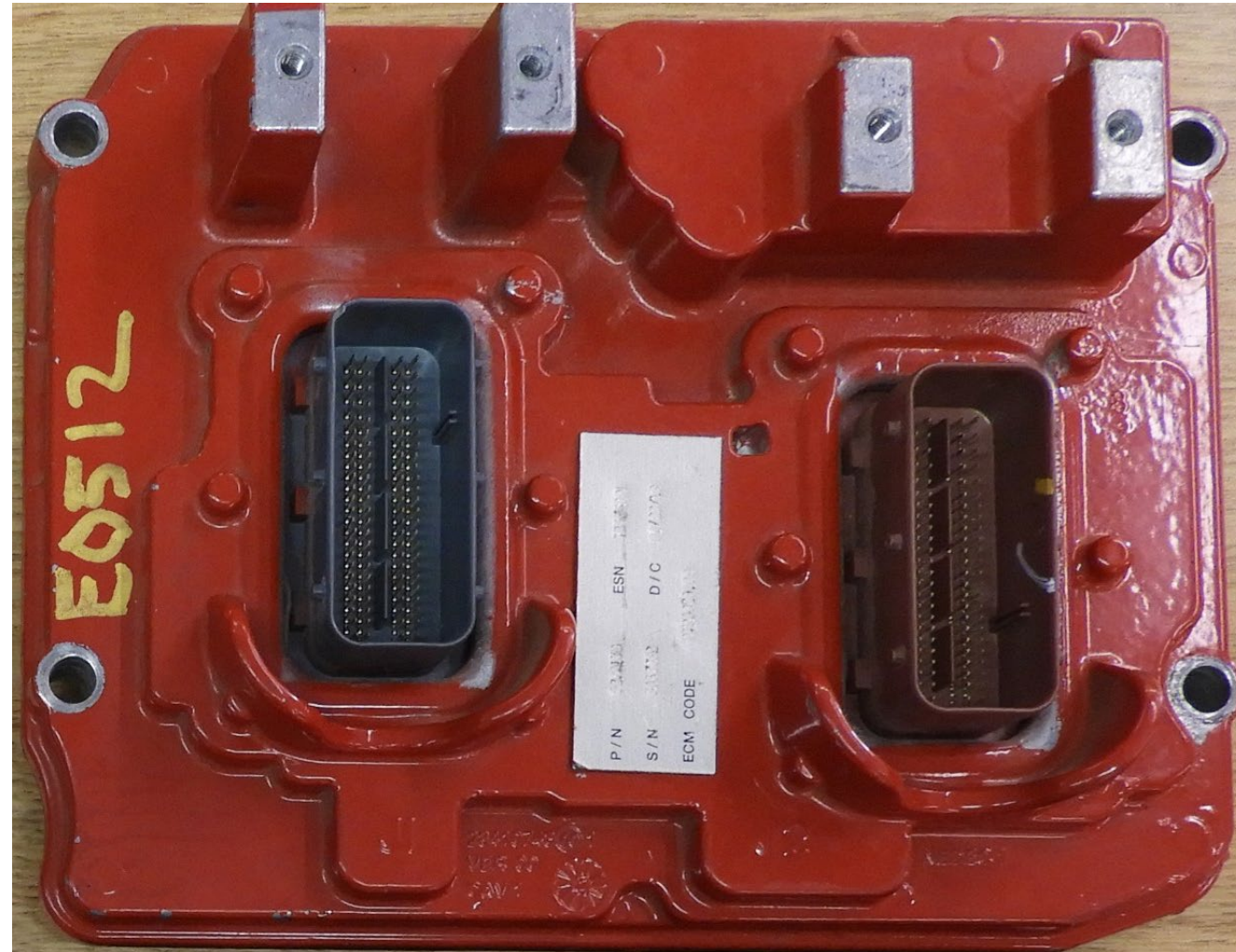
Vehicle Information

Vehicle Identification Number (VIN)	4V4NC9TG25N391063
Vehicle or Equipment Year	
OEM Vehicle Equipment Model	STA15
Customer Name	central
Customer Location	utah
Vehicle Unit Number	25175

```
.....u5..p...).N,.....
.....^CMMNS.....
.....1.1.~!H.....FC0
P388..r.°.....TS.83Û._ÂL..AB10402.22
    ..+.....-
          ..          STA15          4
V4NC9TG25N391063          central
    utah          25175          497294010049729
452003409167300497294340049728955004972882
60049729267004972951800
.xÃnjdb@@0000000000000000000000000000000000..
... . .....d.!..... .....ì.....
```

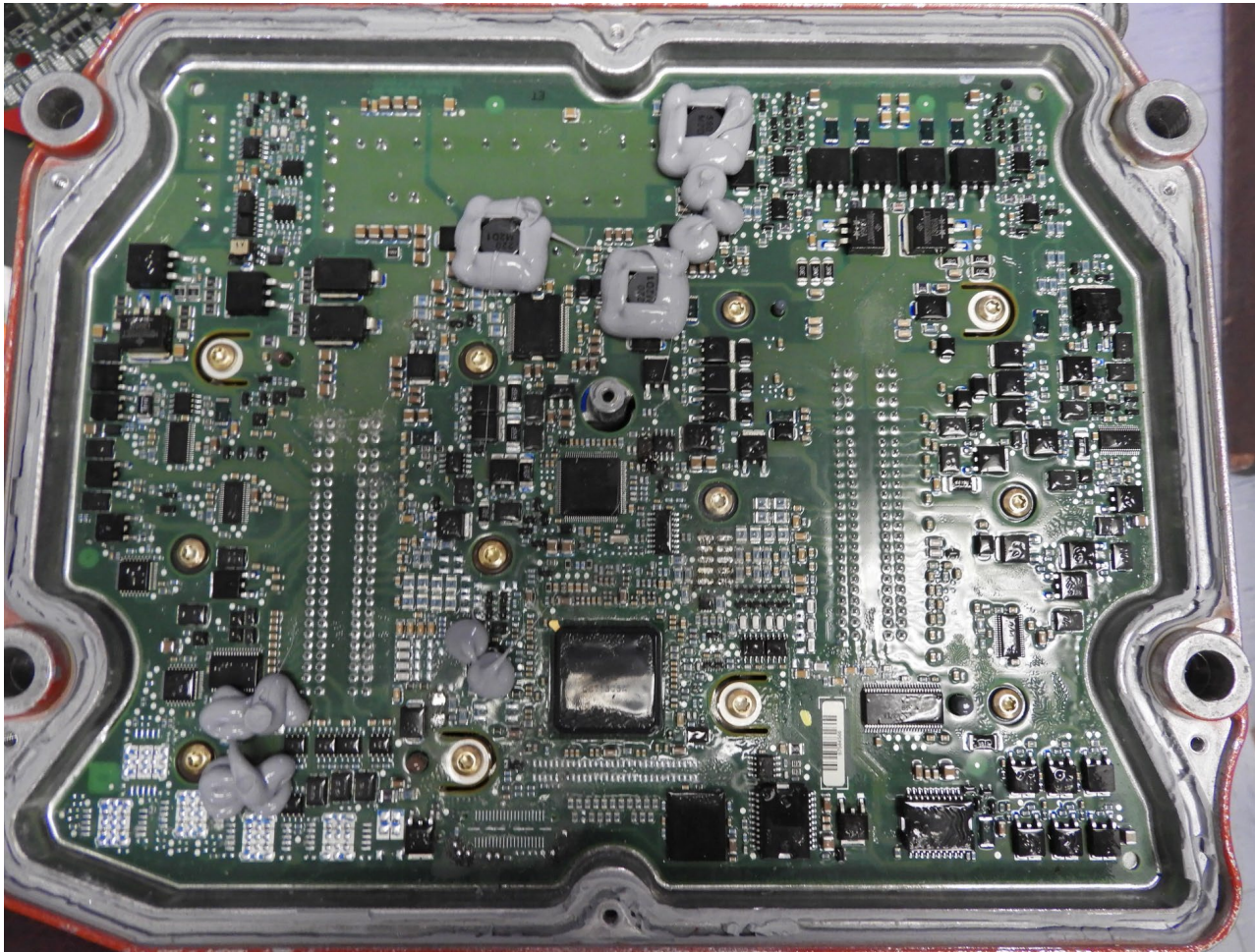
Part of the Hex editor Window

Example for the Cummins CM2350



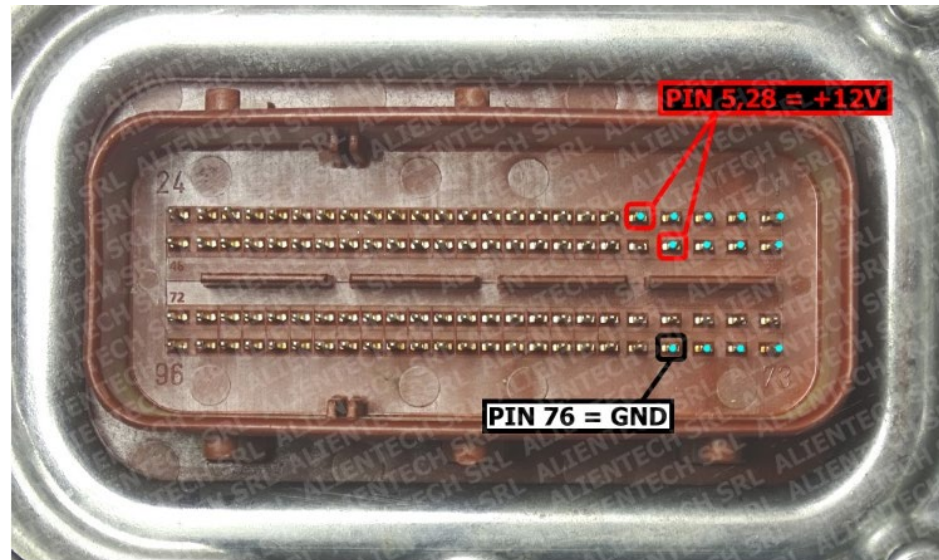
CM2350 Component Identification

Open the ECM to identify JTAG port



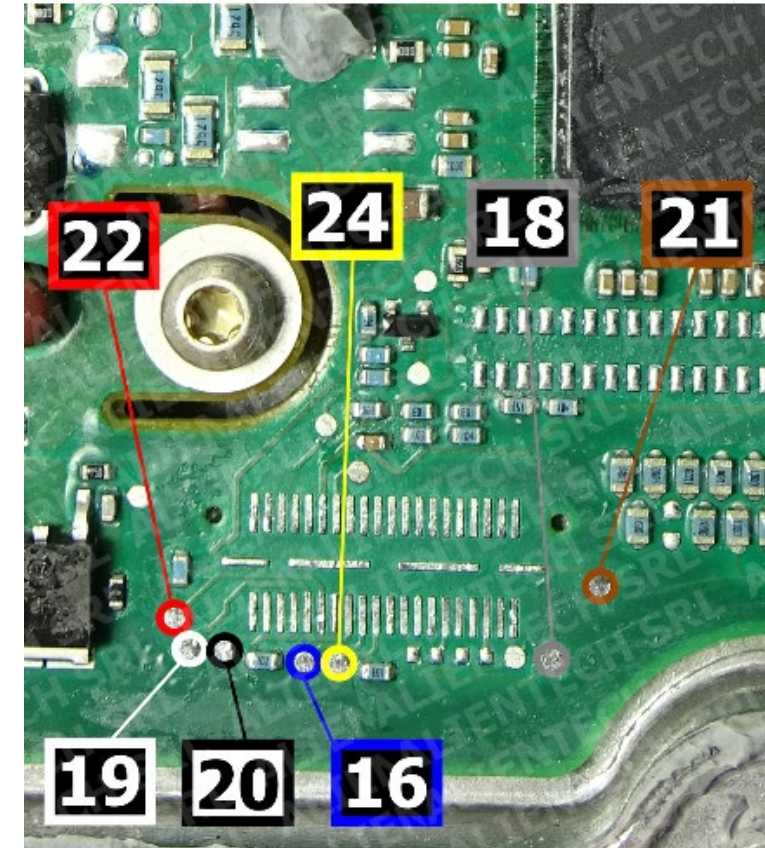
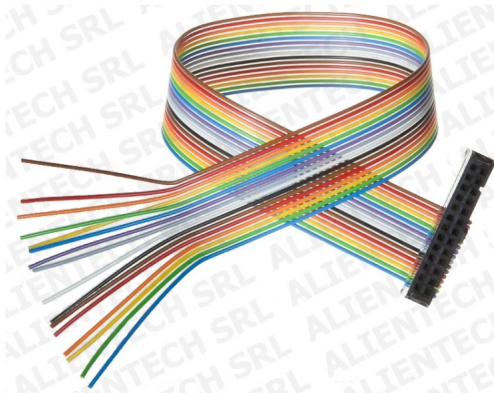
Where is the
JTAG port?

CM2350 Connections from KTAG Software



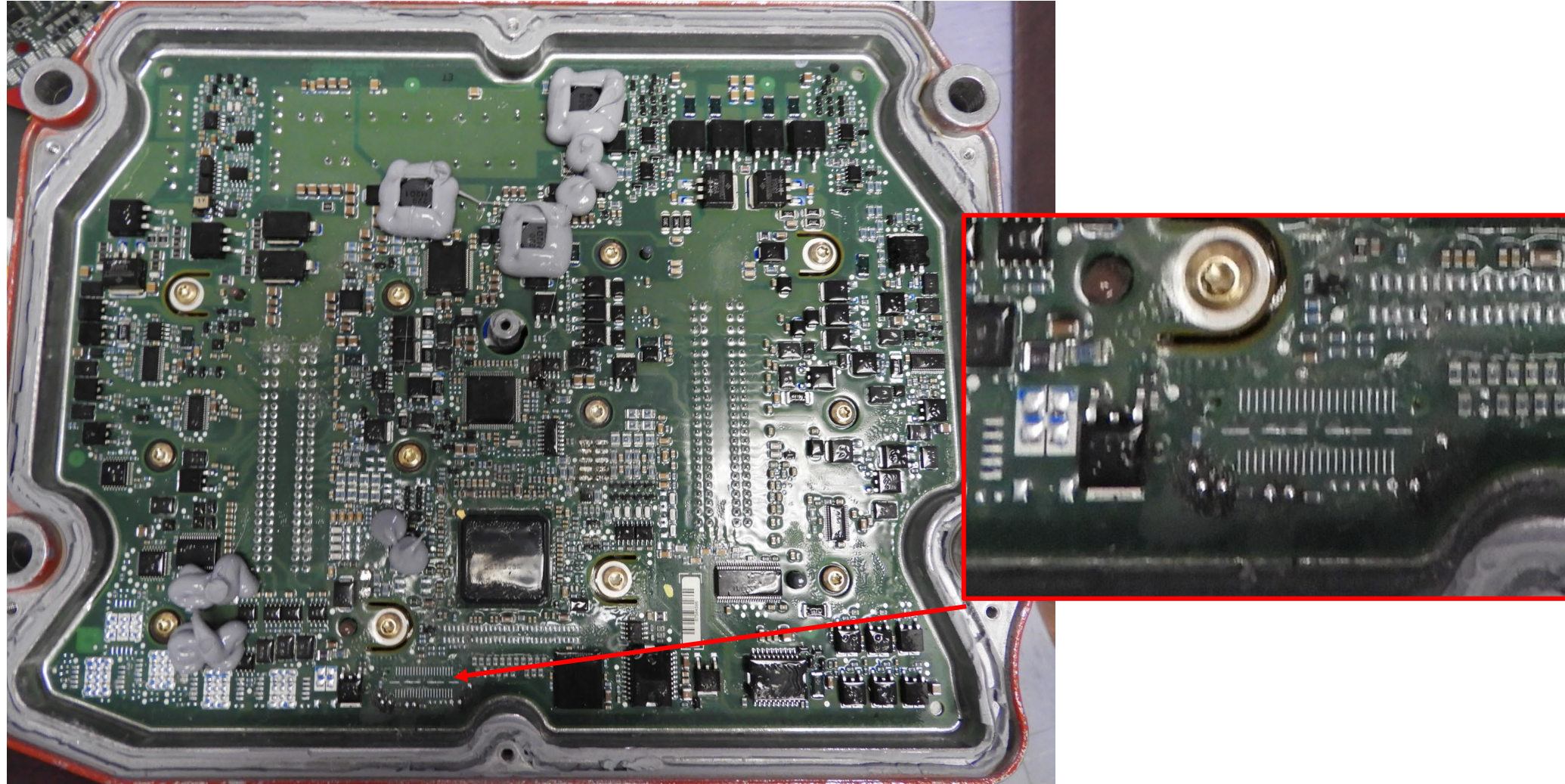
Power, ignition and ground

Ribbon Cable

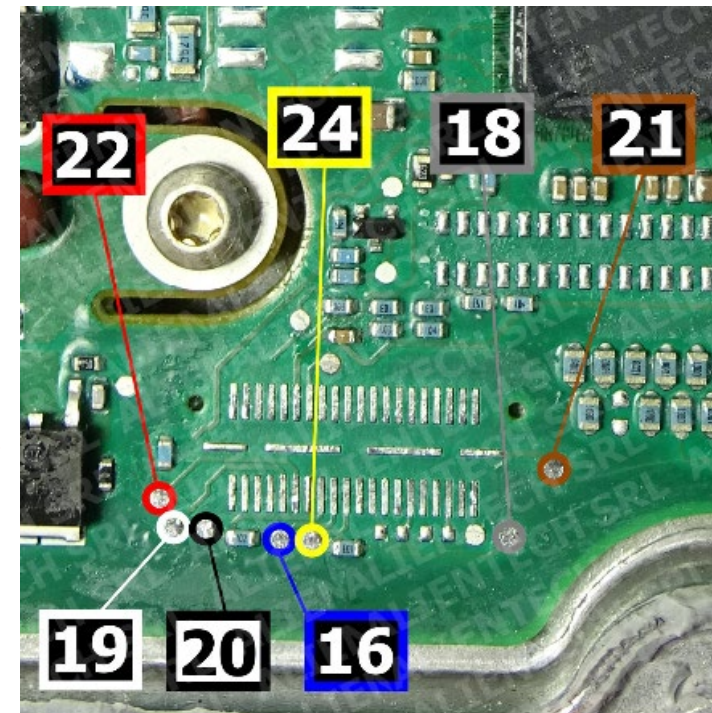
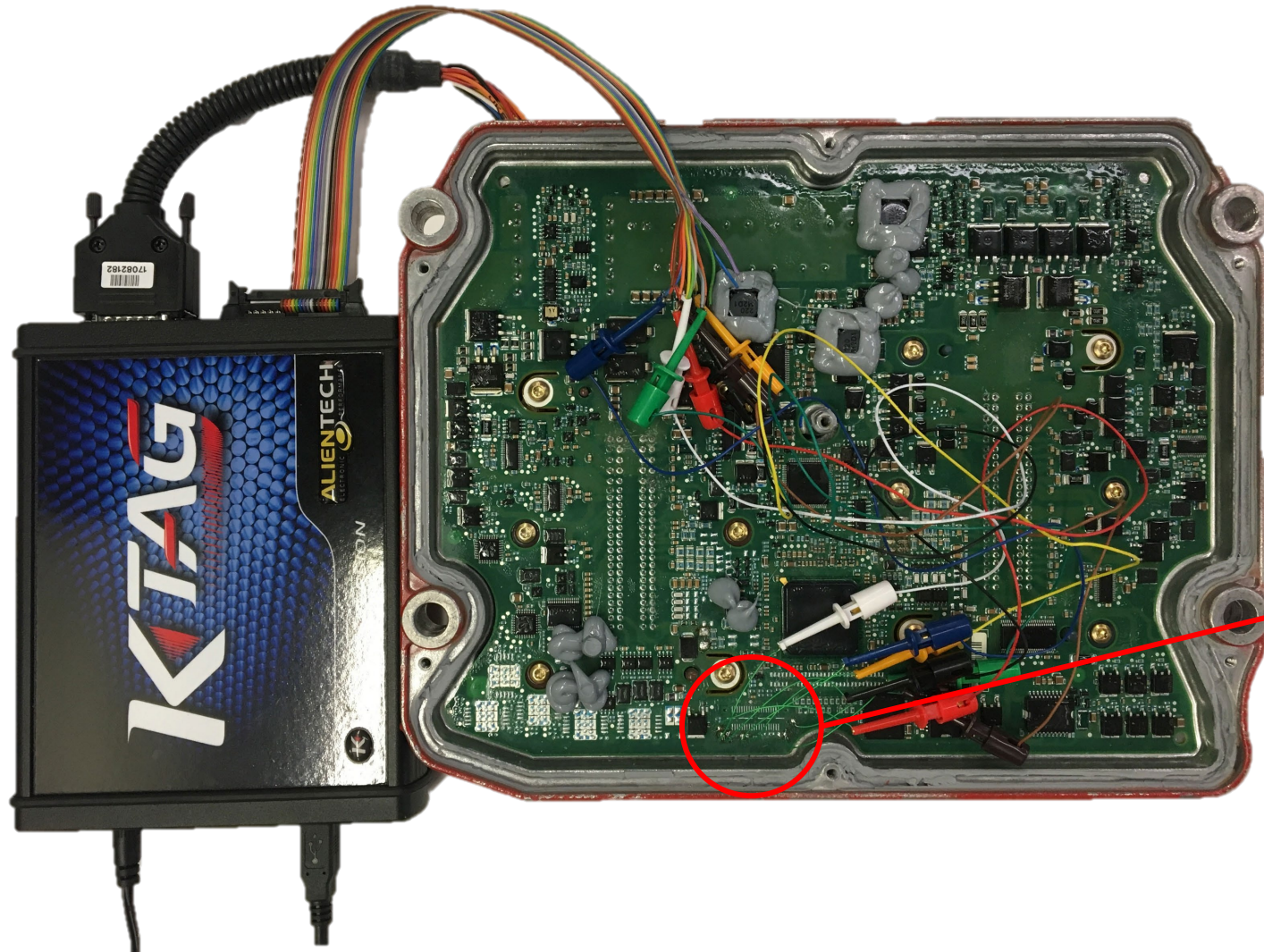


Test Pad Connections

JTAG is built into a Nexus debug port



KTAG Wiring Connections



Summary of Binary Data Collection

CM870

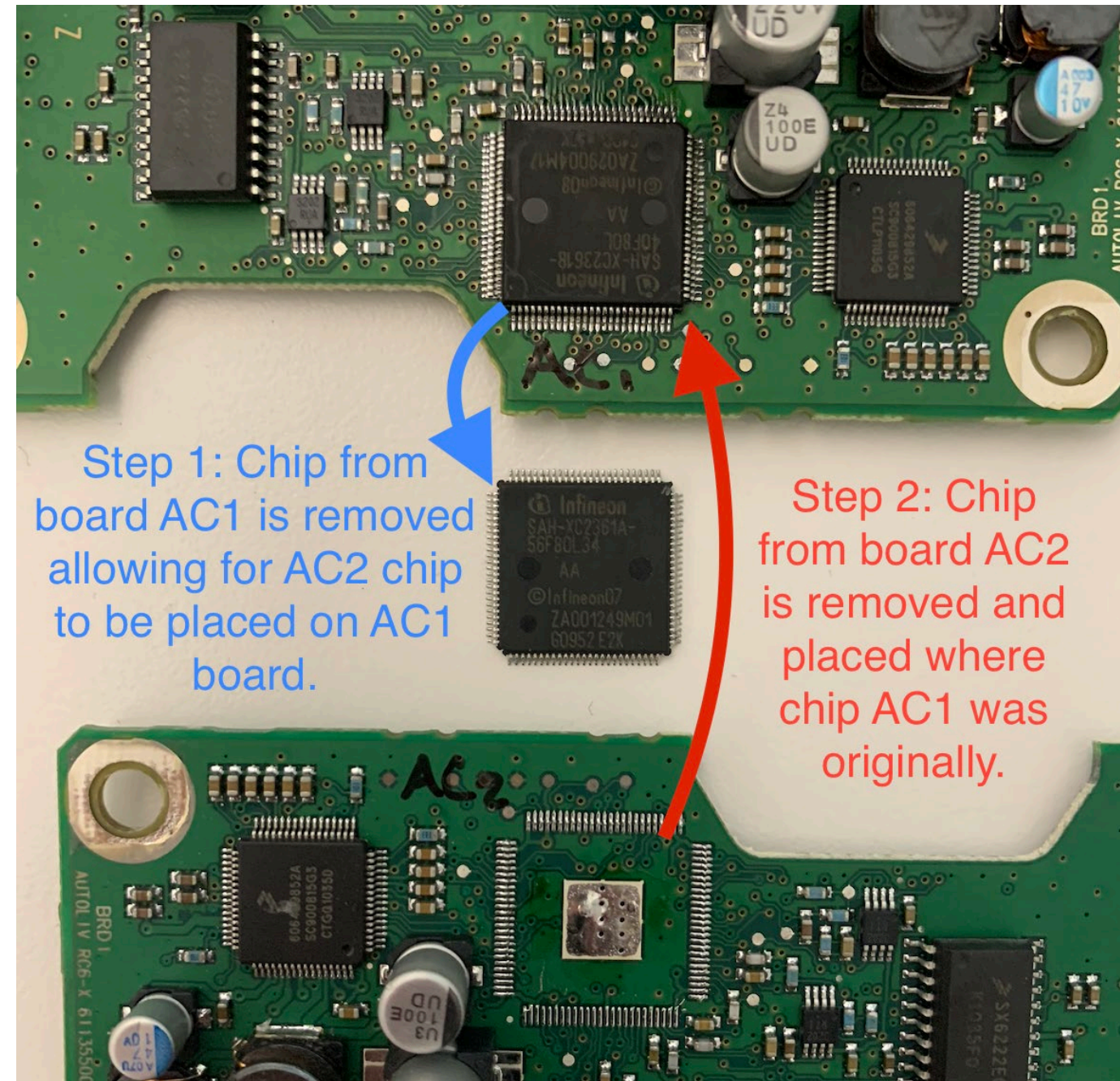
- Three chips
 - Microprocessor
 - External Flash
 - EEPROM (16 kilobytes)
- 1 MB Flash (Intel)
- Flash can be separately extracted with the Xeltek chip reader
- Flex PCB Assembly
- EEPROM contains Data Plate

CM2350

- Single Chip
 - Microprocessor contains flash memory
- 3 MB Flash
- Ball Grid Array
- Non-Standard JTAG Pinout
- Traditional FR4 Printed Circuit Board

Chip Swap

Removing a Chip by Carson Green:
https://youtu.be/q_pJ8OYdXkQ



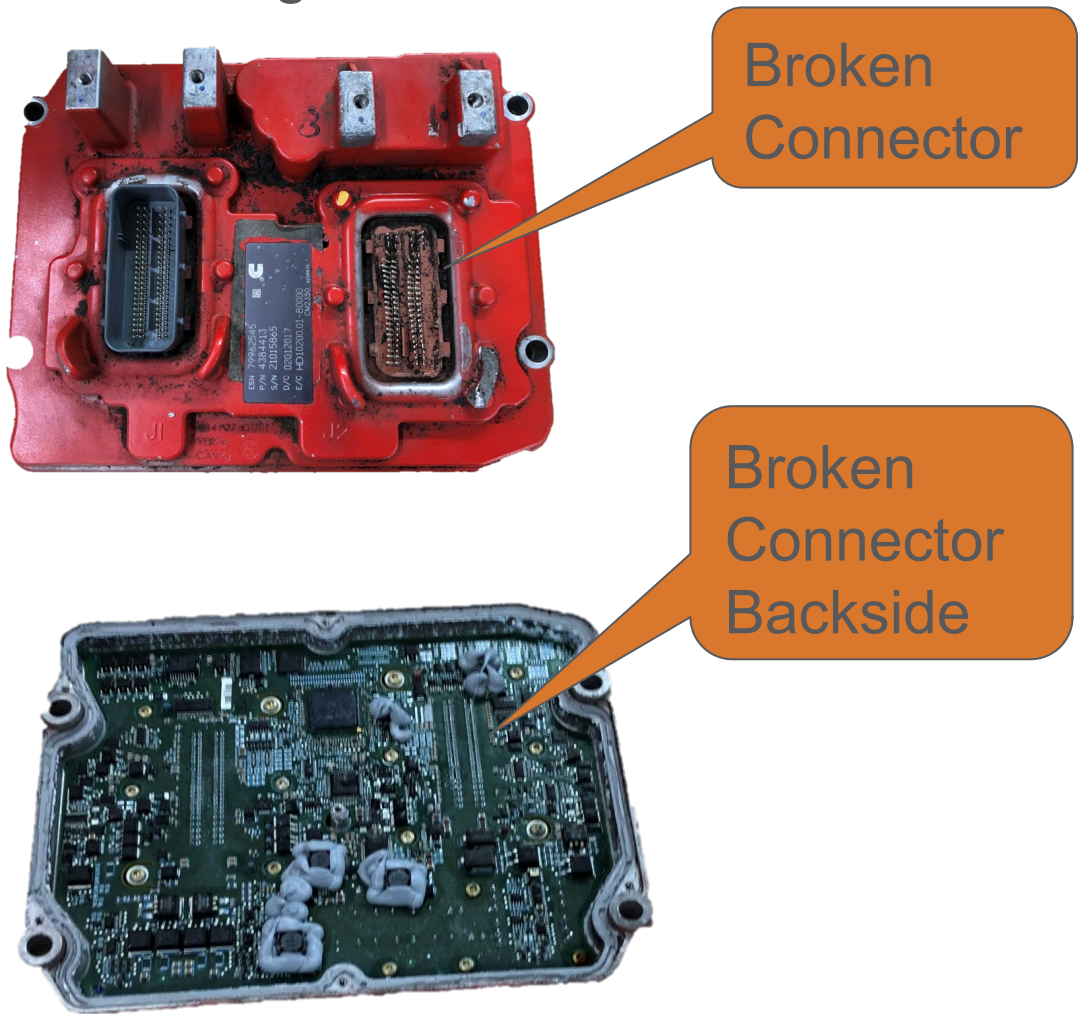
<https://www.youtube.com/channel/UCWaZ7puxImvRRNtnOxc4bAA>

Introducing the Virtual Chip Swap

We can extract data from an ECU, but can we write data back to it?

Cloning an ECU

Damaged ECU

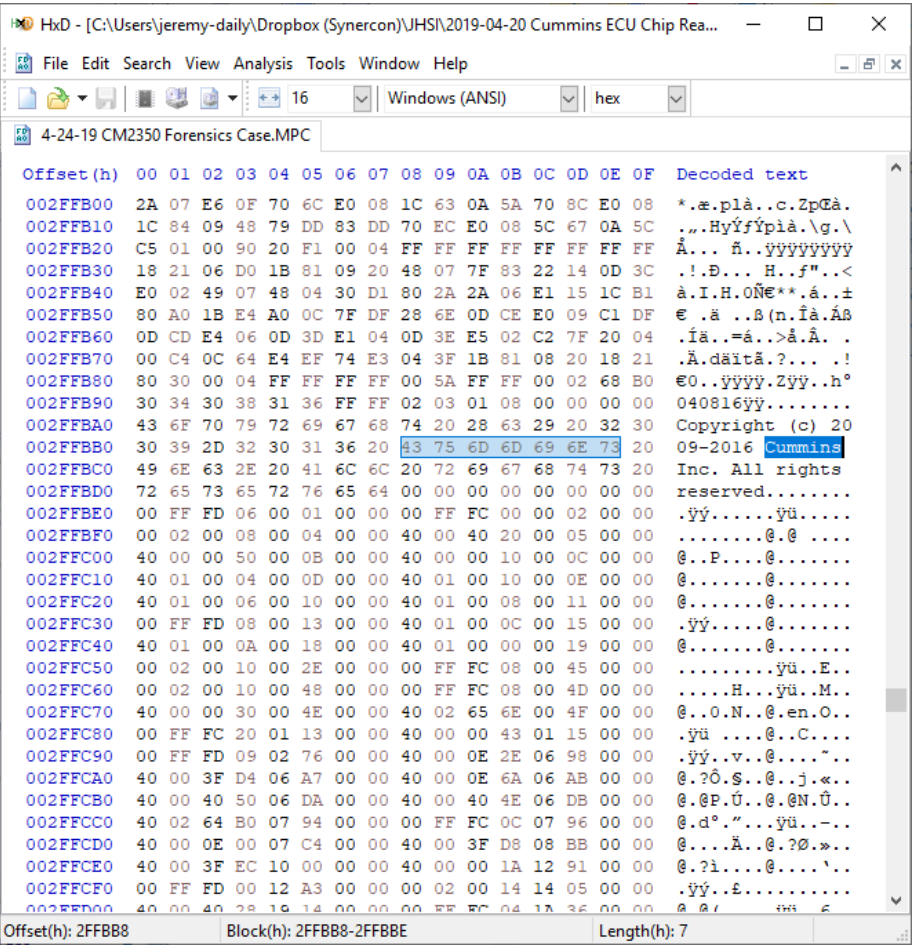


Binary File

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
002FFB00	2A	07	E6	0F	70	6C	E0	08	1C	63	0A	5A	70	8C	E0	08	*.æ.plà..c.ZpEà.
002FFB10	1C	84	09	48	79	DD	83	DD	70	EC	E0	08	5C	67	0A	5C	...HyYfYpià.\g.\
002FFB20	C5	01	00	90	20	F1	00	04	FF	FF	FF	FF	FF	FF	FF	FF	Å... ñ..ýýýýýýýý
002FFB30	18	21	06	D0	1B	81	09	20	48	07	7F	83	22	14	0D	3C	!.Đ... H..f"...<
002FFB40	E0	02	49	07	48	04	30	D1	80	2A	2A	06	E1	15	1C	B1	à.I.H.0Ñε**..á..±
002FFB50	80	A0	1B	E4	A0	0C	7F	DF	28	6E	0D	CE	E0	09	C1	DF	€ .ä ...ß(n.ia.Åß
002FFB60	0D	CD	E4	06	0D	3D	E1	04	0D	3E	E5	02	C2	7F	20	04	.ia...=á...>ã.Å. .
002FFB70	00	C4	0C	64	E4	EF	74	E3	04	3F	1B	81	08	20	18	21	.Å.däitã.?... .!
002FFB80	80	30	00	04	FF	FF	FF	FF	00	5A	FF	FF	00	02	68	B0	€0..ýýýý.Zýý..h°
002FFB90	30	34	30	38	31	36	FF	FF	02	03	01	08	00	00	00	00	040816ýý.....
002FFBA0	43	6F	70	79	72	69	67	68	74	20	28	63	29	20	32	30	Copyright (c) 20
002FFBB0	30	39	2D	32	30	31	36	20	43	75	6D	6D	69	6E	73	20	09-2016 Cummins
002FFBC0	49	6E	63	2E	20	41	6C	6C	20	72	69	67	68	74	73	20	Inc. All rights
002FFBD0	72	65	73	65	72	76	65	64	00	00	00	00	00	00	00	00	reserved.....
002FFBE0	00	FF	FD	06	00	01	00	00	00	FF	FC	00	00	02	00	00	.ýý.....ýü.....
002FFBF0	00	02	00	08	00	04	00	00	40	00	40	20	00	05	00	00@.@
002FFC00	40	00	00	50	00	0B	00	00	40	00	00	10	00	0C	00	00	@..P....@.....
002FFC10	40	01	00	04	00	0D	00	00	40	01	00	10	00	0E	00	00	@.....@.....
002FFC20	40	01	00	06	00	10	00	00	40	01	00	08	00	11	00	00	@.....@.....
002FFC30	00	FF	FD	08	00	13	00	00	40	01	00	0C	00	15	00	00	.ýý.....@.....
002FFC40	40	01	00	0A	00	18	00	00	40	01	00	00	00	19	00	00	@.....@.....
002FFC50	00	02	00	10	00	2E	00	00	FF	FC	08	00	45	00	00	00ýü..E..
002FFC60	00	02	00	10	00	48	00	00	FF	FC	08	00	4D	00	00	00H...ýü..M..
002FFC70	40	00	00	30	00	4E	00	00	40	02	65	6E	00	4F	00	00	@..O.N...@.en.O..
002FFC80	00	FF	FC	20	01	13	00	00	40	00	00	43	01	15	00	00	.ýü....@..C....
002FFC90	00	FF	FD	09	02	76	00	00	40	00	0E	2E	06	98	00	00	.ýý..v...@.....
002FFCA0	40	00	3F	D4	06	A7	00	00	40	00	0E	6A	06	AB	00	00	@.?Ö.Ş...@..j.«.
002FFCB0	40	00	40	50	06	DA	00	00	40	00	40	4E	06	DB	00	00	@.@P.Ú...@.@N.Ů..
002FFCC0	40	02	64	B0	07	94	00	00	FF	FC	0C	07	96	00	00	00	@.d°..."ýü...-
002FFCD0	40	00	0E	00	07	C4	00	00	40	00	3F	D8	08	BB	00	00	@...Ä...@.?Ø.»..
002FFCE0	40	00	3F	EC	10	00	00	00	40	00	00	1A	12	91	00	00	@.?ì....@.....
002FFCF0	00	FF	FD	00	12	A3	00	00	02	00	14	14	05	00	00	00	.ýý..£.....
002FFD00	40	00	40	28	18	14	00	00	FF	FC	04	1A	36	00	00	00	@. / ...titi 6

Cloning Process

Binary File



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
002FFB00 2A 07 E6 0F 70 6C E0 08 1C 63 0A 5A 70 8C E0 08 *.æ.plà..c.ZpCà.
002FFB10 1C 84 09 48 79 DD 83 DD 70 EC E0 08 5C 67 0A 5C ...HyYfYplà.\g.\
002FFB20 C5 01 00 90 20 F1 00 04 FF FF FF FF FF FF FF FF Å... å..yyyyyyyy
002FFB30 18 21 06 D0 1B 81 09 20 48 07 7F 83 22 14 0D 3C !.D... H..f"...<
002FFB40 E0 02 49 07 48 04 30 D1 80 2A 2A 06 E1 15 1C B1 à.I.H.0Ñe**.á.±
002FFB50 80 A0 1B E4 A0 0C 7F DF 28 6E 0D CE E0 09 C1 DF € .ä .B(n.îà.ÁB
002FFB60 0D CD E4 06 0D 3D E1 04 0D 3E E5 02 C2 7F 20 04 .îä..=ä..>â.Â. .
002FFB70 00 C4 0C 64 E4 EF 74 E3 04 3F 1B 81 08 20 18 21 .Ä.däitâ.?... !!
002FFB80 80 30 00 04 FF FF FF FF 00 5A FF FF 00 02 68 B0 e0..ýýýý.Zýý..h°
002FFB90 30 34 30 38 31 36 FF FF 02 03 01 08 00 00 00 00 040816ýý.....
002FFBA0 43 6F 70 79 72 69 67 68 74 20 28 63 29 20 32 30 Copyright (c) 20
002FFBB0 30 39 2D 32 30 31 36 20 43 75 6D 6D 69 6E 73 20 09-2016 Cummins
002FFBC0 49 6E 63 2E 20 41 6C 6C 20 72 69 67 68 74 73 20 Inc. All rights
002FFBD0 72 65 73 65 72 76 65 64 00 00 00 00 00 00 00 00 reserved.....
002FFBE0 00 FF FD 06 00 01 00 00 00 FF FC 00 00 02 00 00 .ýý.....ýü.....
002FFBF0 00 02 00 08 00 04 00 00 40 00 40 20 00 05 00 00 .....@.@ .....
002FFC00 40 00 00 50 00 08 00 00 40 00 00 10 00 0C 00 00 @..P....@.....
002FFC10 40 01 00 04 00 0D 00 00 40 01 00 10 00 0E 00 00 @.....@.....
002FFC20 40 01 00 06 00 10 00 00 40 01 00 08 00 11 00 00 @.....@.....
002FFC30 00 FF FD 08 00 13 00 00 40 01 00 0C 00 15 00 00 .ýý.....@.....
002FFC40 40 01 00 0A 00 18 00 00 40 01 00 00 00 19 00 00 @.....@.....
002FFC50 00 02 00 10 00 2E 00 00 00 FF FC 08 00 45 00 00 .....ýü..E..
002FFC60 00 02 00 10 00 48 00 00 00 FF FC 08 00 4D 00 00 .....H...ýü..M..
002FFC70 40 00 00 30 00 4E 00 00 40 02 65 6E 00 4F 00 00 @..O.N..@.en.O..
002FFC80 00 FF FC 20 01 13 00 00 40 00 00 43 01 15 00 00 .ýü ....@..C....
002FFC90 00 FF FD 09 02 76 00 00 40 00 0E 2E 06 98 00 00 .ýý..v...@.....~..
002FFCA0 40 00 3F D4 06 A7 00 00 40 00 0E 6A 06 AB 00 00 @.?Ö.$..@.j.«..
002FFCB0 40 00 40 50 06 DA 00 00 40 00 40 4E 06 DB 00 00 @.@P.Ú..@.N.Ů..
002FFCC0 40 02 64 B0 07 94 00 00 00 FF FC 0C 07 96 00 00 @.d°..."ýü..-..
002FFCD0 40 00 0E 00 07 C4 00 00 40 00 3F D8 08 BB 00 00 @....Ä..@.?Ö»..
002FFCE0 40 00 3F EC 10 00 00 00 40 00 00 1A 12 91 00 00 @.?ì.....@.....\..
002FFCF0 00 FF FD 00 12 A3 00 00 00 02 00 14 14 05 00 00 .ýý..£.....
002FFD00 40 00 40 28 18 14 00 00 00 FF FC 04 1A 36 00 00 @ @ /
```

Load Binary onto working ECU;
Perform a bench download



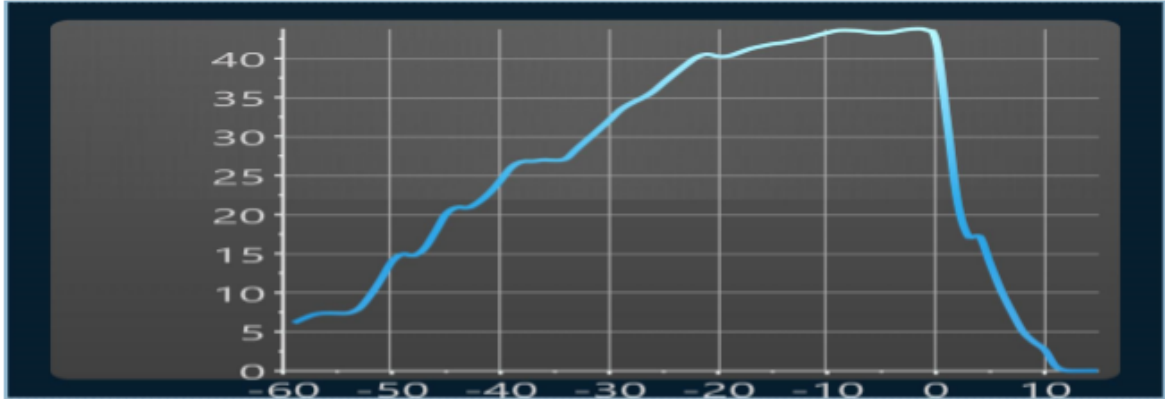
Interpret Data from ECU after Cloning

- After cloning the ECU, download with traditional benchtop methods
- Example: Cummins PowerSpec with a DPA5 connected to a Smart Sensor Simulator 2

Sudden Vehicle Speed Deceleration Report Record 1

Engine Type	ISX 2010	Ecm Code	CL10132.39
Engine Serial Number	60811136	Software Phase	7.70.0.71
Unit Number	0000000000	Extraction Date	04-03-2019 04:37:51
Sudden Decel Threshold Rate:	N/A	ECM Run time	8227:56:32
Occurrence Date: N/A		ECM Run Time at Occurrence: 2899:18:36	
Air Temperature (°F) at Occurrence: 72		Occurrence Distance (mi): 109323.4	

Vehicle Speed

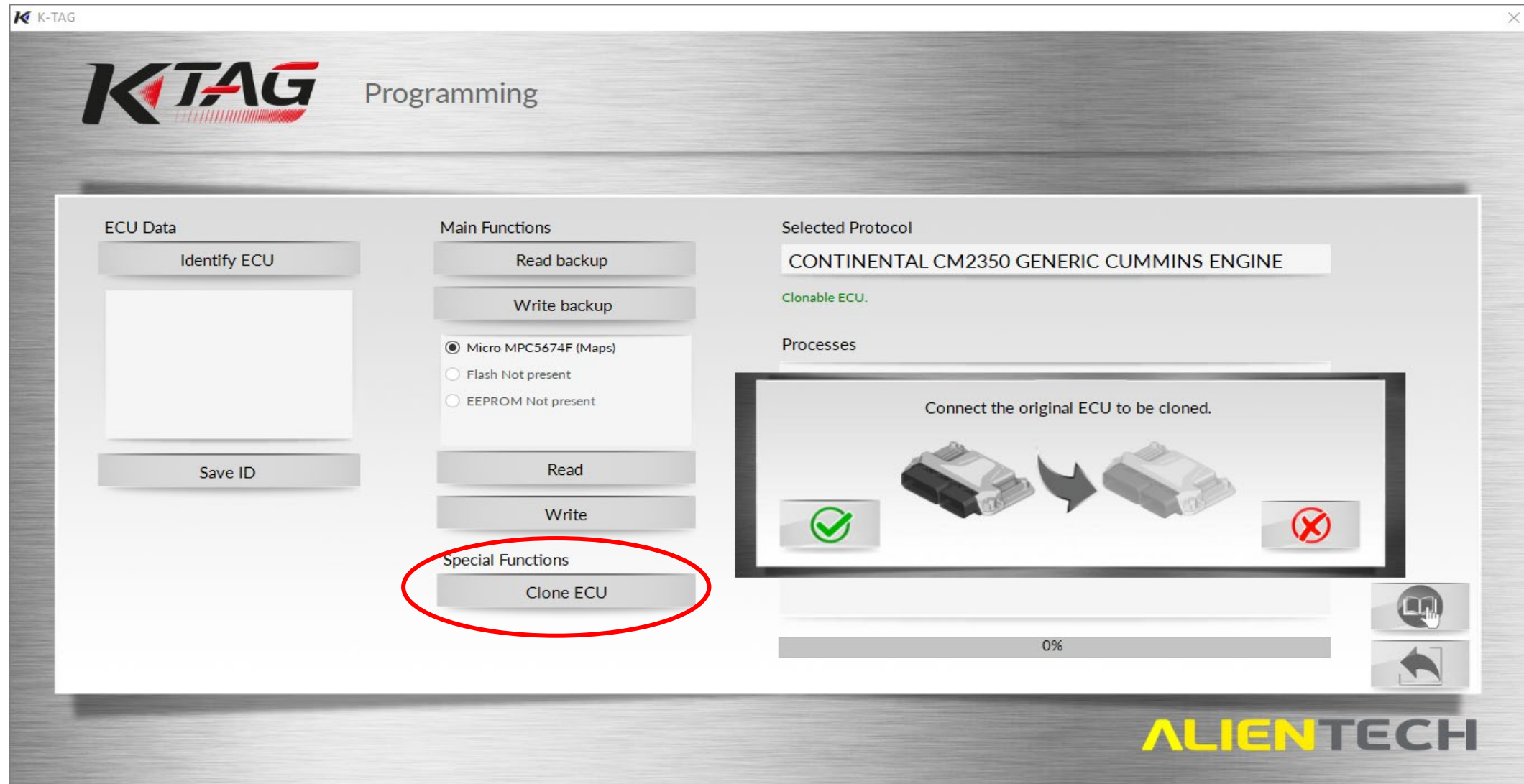


Record 1

Time (Seconds)	Vehicle Speed (mph)	Engine Speed (rpm)	Engine Load (%)	Throttle (%)	Brake Status	Clutch Status	Cruise Status	Lamp Status
-59	6	683	34.8	30.1	-	-	-	-
-58	7	788	33.6	32.2	-	-	-	-
-57	7	813	21.9	27.5	-	-	-	-

Cloning Process with the K-TAG

Select Clone ECU function and follow instructions



Cloning Example: Two Different ECUs

Engine Dataplate Report				Engine Dataplate Report			
Engine Type	ISX 2013	Ecm Code	EF10067.36	Engine Type	ISB 2013	Ecm Code	DT90216.08
Engine Serial Number	0	Software Phase	9.40.13.61	Engine Serial Number	73993334	Software Phase	21.60.71.2
Unit Number	0000000000	Extraction Date	07-03-2018 12:37:22	Unit Number	*****	Extraction Date	07-03-2018 12:14:56

ECM Information		ECM Information	
Module Name	CM2350	Module Name	CM2350
Ecm Code	EF10067.36	Ecm Code	DT90216.08
Software Phase	9.40.13.61	Software Phase	21.60.71.2
ECM Serial Number	3032682	ECM Serial Number	6069868
ECM Part Number	5290170	ECM Part Number	4358814

Engine Information		Engine Information	
Engine Model	ISX 2013	Engine Model	ISB 2013
Engine Build Date	010185	Engine Build Date	110516
Engine Serial Number	0	Engine Serial Number	73993334
Do Option	1874	Do Option	94370
SC Option	12186	SC Option	92050

Vehicle Information		Vehicle Information	
Vehicle Identification Number (VIN)	1HSDJAPR7EH784086	Vehicle Identification Number (VIN)	2NKHHM7X3HM156651
Vehicle or Equipment Year	2014	Vehicle or Equipment Year	*****
OEM Vehicle Equipment Model	*****	OEM Vehicle Equipment Model	1300
Customer Name	CustomerName**	Customer Name	CustomerName**
Customer Location	*****	Customer Location	*****
Vehicle Unit Number	0000000000	Vehicle Unit Number	*****

Extraction Date
not in ECU

A

B

ECM dataplate of the two ECUs **before** cloning

Cloning Results: A is now B

Engine Dataplate Report				Engine Dataplate Report			
Engine Type	ISB 2013	Ecm Code	DT90216.08	Engine Type	ISB 2013	Ecm Code	DT90216.08
Engine Serial Number	73993334	Software Phase	21.60.71.2	Engine Serial Number	73993334	Software Phase	21.60.71.2
Unit Number	*****	Extraction Date	07-03-2018 03:51:29	Unit Number	*****	Extraction Date	07-03-2018 12:14:56
ECM Information				ECM Information			
Module Name	CM2350	ECM Serial Number	6069868	Module Name	CM2350	ECM Serial Number	6069868
Ecm Code	DT90216.08	ECM Part Number	4358814	Ecm Code	DT90216.08	ECM Part Number	4358814
Software Phase	21.60.71.2			Software Phase	21.60.71.2		
Engine Information				Engine Information			
Engine Model	ISB 2013	Engine Build Date	110516	Engine Model	ISB 2013	Engine Build Date	110516
Engine Serial Number	73993334	Do Option	94370	Engine Serial Number	73993334	Do Option	94370
Do Option	94370	SC Option	92050	Do Option	94370	SC Option	92050
SC Option	92050			SC Option	92050		
Vehicle Information				Vehicle Information			
Vehicle Identification Number (VIN)	2NKHHM7X3HM156651	Vehicle or Equipment Year	T300	Vehicle Identification Number (VIN)	2NKHHM7X3HM156651	Vehicle or Equipment Year	T300
Vehicle or Equipment Year	*****	Customer Name	*****	Vehicle or Equipment Year	*****	Customer Name	*****
OEM Vehicle Equipment Model	T300	Customer Location	*****	OEM Vehicle Equipment Model	T300	Customer Location	*****
Customer Name	CustomerName**	Vehicle Unit Number	*****	Customer Name	CustomerName**	Vehicle Unit Number	*****
Customer Location	*****			Customer Location	*****		
Vehicle Unit Number	*****			Vehicle Unit Number	*****		

ECM dataplate of the two ECMs **after** cloning



Data Analysis

What if cloning doesn't work (or you don't want to spend the money on another ECU)?

Data Analysis: Human Readable Text

Some meaningful strings are present indicating that the data is not encrypted

0	00	48	00	03	AE	..H..U.....H.....H.....H.....H..@
0	00	00	00	48	00H.....H.....H.....H.....H.
4	82	00	00	00	00H.....H.....H.....H.....
8	00	04	82	00	00	H.....H.....H.....H.....H.....
0	00	48	00	04	82	..H.....H.....H.....H.....H...
0	00	28	D0	00	00H.....H.....H.....H..(Ò..(Ð..
0	01	09	02	2E	00	..121802.... ..ÿÿÿ@p
7	05	07	02	40	00	...À.. ..ÿÿÿ.....@.....@.....@.
3	20	49	6E	63	2E@... ..Cummins Inc...Cummins Inc.
5	72	65	64	20	77	Engine Control Module..Self-powered w
E	20	66	6F	72	20	ith one Interface.Bulk connection for
8	C6	97	A3	80	E6	applications..ÿÿ.!ÿØ,<À.±8Æ.£.æ
A	14	2C	05	00	02	...F.. .PP,...@.. 8 ÿpH...8 .p ±*.,...
8	E0	00	64	48	00	@..'.'á. .á..... 9..... ,...@.. 8à.dH.
0	14	3D	80	00	01	.<,...@.. 8à.tH...8à.u,...@...H...=...
9	41	00	0B	39	4A	9..Ð}c... 1Z.=..±°l.....9`...l...A. 9J
0	02	99	8A	00	00	...A.ì...a. 9k...a. .A. 9.....
C	08	03	A6	38	21	..!. .&...a...f..9@...C..H..}...., .. 8!
2	76	90	01	00	14	/M .. 1±°

Data Analysis: Binary File

- Flash chip data should carry Sudden Deceleration information (vehicle speed, engine RPM, etc.)
- The file is 3 MB so how can we locate the Sudden Decel?

```
000001FF70  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.....
000001FF80  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.....
000001FF90  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.....
000001FFA0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.....
000001FFB0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.....
000001FFC0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.....
000001FFD0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.....
000001FFE0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.....
000001FFF0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.....
0000020000  94 21 FF F0 7C 08 02 A6-93 E1 00 0C 90 01 00 14  .!..
|  .
. .
0000020010  3F E0 00 B2 A3 FF 5B 96-3C E0 00 B2 38 E7 30 BA
?.....[.<...8.0.
0000020020  7C E6 3B 78 3D 00 00 B2-39 08 30 B8 7D 05 43 78
|.;x=...90.}|Cx
0000020030  3D 20 00 B1 A1 29 E3 74-7C 09 F8 00 41 81 00 1C  =
...).t|  ..A..
0000020040  39 80 20 00 B1 88 00 00-3C 80 00 B1 A0 84 E3 76  9.
.....<.....v
0000020050  B0 87 00 00 48 00 00 24-3C 80 00 B1 A0 84 E3 70
....H..$<.....p
0000020060  B0 88 00 00 3D 00 00 B1-A1 08 E3 72 B1 07 00 00  ....
=......r.  ..
0000020070  7D 44 40 50 38 8A 20 00-3D 80 00 B2 B0 8C 30 BC  }
D@P8.  .=.....0.
0000020080  3C E0 00 B2 A0 E7 62 68-A1 45 00 00 7D 07 51 D6
<.....bh.E..} Q.
0000020090  3C A0 00 B0 38 A5 5A 58-A1 65 00 00 A1 26 00 00
<...8.ZX.e...&..
00000200A0  7C 6B 49 D6 3C C0 00 B0-38 C6 5A 5A A1 46 00 00  |kI.
<...8.ZZ.F..
00000200B0  54 89 04 3E 7C 8A 49 D6-7D 83 40 50 7D 04 62 14  T.}>
|.I.}.@P}^b||
00000200C0  2C 08 00 00 40 81 00 2C-7D 08 6E 70 3D 60 00 00  ,.
@...}np=`..
00000200D0  61 6B 8C A0 7C 08 58 00-40 80 00 0C 7D 04 43 78  ak..
|X.@..
```


Data Analysis

One approach:

- Observe that vehicle speed for Record 1 in this ECM has 150 mph for the first 60s.
- There should be repeated data in the binary.

Record 1

Time (Seconds)	Vehicle Speed (mph)	Engine Speed (rpm)	Engine Load (%)	Throttle (%)	Brake Status	Clutch Status	Cruise Status	Lamp Status
-59	150	0	0.0	0.0	-	-	-	On
-58	150	0	0.0	0.0	-	-	-	On
-57	150	0	0.0	0.0	-	-	-	On
-56	150	0	0.0	0.0	-	-	-	On
-55	150	0	0.0	0.0	-	-	-	On
-54	150	0	0.0	0.0	-	-	-	On
-53	150	0	0.0	0.0	-	-	-	On
-52	150	0	0.0	0.0	-	-	-	On
-51	150	0	0.0	0.0	-	-	-	On
-50	150	0	0.0	0.0	-	-	-	On
-49	150	0	0.0	0.0	-	-	-	On
-48	150	0	0.0	0.0	-	-	-	On
-47	150	0	0.0	0.0	-	-	-	On
-46	150	0	0.0	0.0	-	-	-	On
-45	150	0	0.0	0.0	-	-	-	On
-44	150	0	0.0	0.0	-	-	-	On
-43	150	0	0.0	0.0	-	-	-	On
-42	150	0	0.0	0.0	-	-	-	On
-41	150	0	0.0	0.0	-	-	-	On
-40	150	0	0.0	0.0	-	-	-	On
-39	150	0	0.0	0.0	-	-	-	On
-38	150	0	0.0	0.0	-	-	-	On
-37	150	0	0.0	0.0	-	-	-	On

Data Analysis

Converting the actual vehicle speed from the report to raw data format using SAE J1939-71

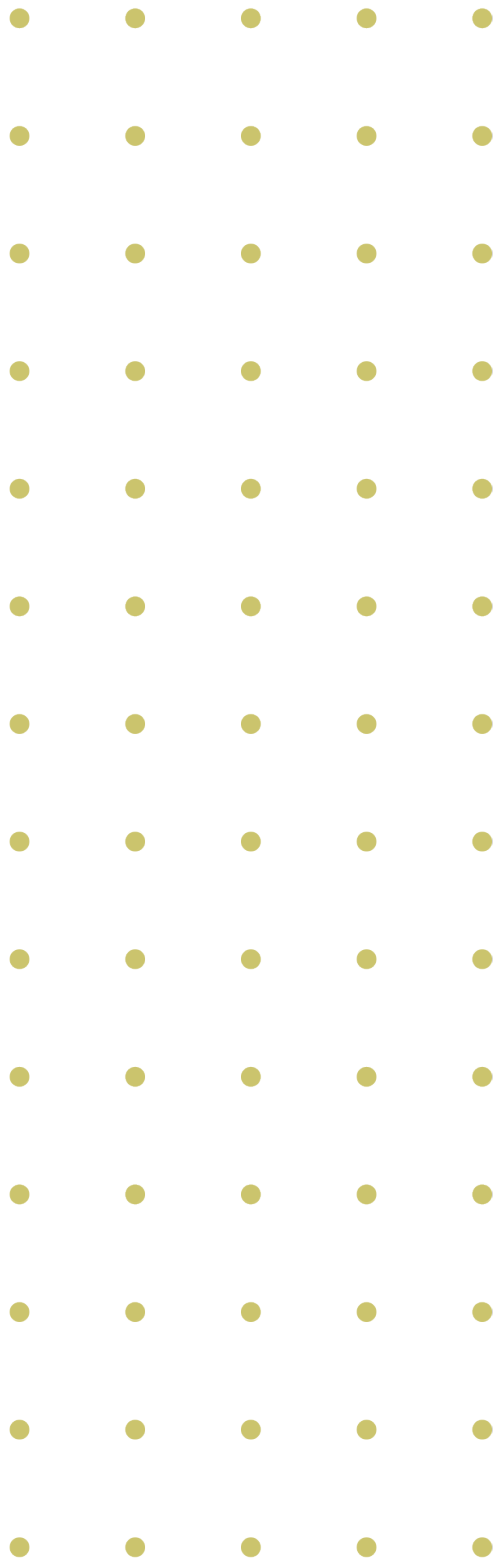
SPN 84 Wheel-Based Vehicle Speed

Speed of the vehicle as calculated from wheel or tailshaft speed.

Data Length:	2 bytes	
Resolution:	1/256 km/h per bit, 0 offset	
Data Range:	0 to 250.996 km/h	Operational Range: same as data range
Type:	Measured	
Supporting Information:		
PGN reference:	65265	

Data Analysis Approach

- Convert 150 mph to km/h: 241.4 km/h
- Convert 241.4 km/h to bit:
 $241.4 \text{ km/h} \times 256 \text{ bit/km/h} = 64798$
- Convert 64798 to Hex: F1 66
- Look for repeating F1 66 pattern in the report



NO PATTERN! WHAT NOW?!

Data Analysis

- Convert 150 mph to data format without converting to km/h
- Convert 150.000 to hex:
 $150 * 256 = 38,400$
- Convert 38,400 to Hex: 96 00

Data Analysis

We got something!

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0x0FB1D0	00	00	00	00	00	00	00	00	0C	31	00	00	00	00	00	00 1.....
0x0FB1E0	00	00	00	73	00	02	1E	FA	15	9B	85	8A	12	F6	01	D2	...s.. ú.....ö.Ò
0x0FB1F0	79	DC	00	00	96	00	00	00	00	00	00	00	00	00	00	01	yÜ.....
0x0FB200	00	00	96	00	00	00	00	00	00	00	00	00	00	01	00	00
0x0FB210	96	00	00	00	00	00	00	00	00	00	00	01	00	00	96	00
0x0FB220	00	00	00	00	00	00	00	00	00	01	00	00	96	00	00	00
0x0FB230	00	00	00	00	00	00	00	01	00	00	96	00	00	00	00	00
0x0FB240	00	00	00	00	00	01	00	00	96	00	00	00	00	00	00	00
0x0FB250	00	00	00	01	00	00	96	00	00	00	00	00	00	00	00	00
0x0FB260	00	01	00	00	96	00	00	00	00	00	00	00	00	00	00	01
0x0FB270	00	00	96	00	00	00	00	00	00	00	00	00	00	01	00	00
0x0FB280	96	00	00	00	00	00	00	00	00	00	00	01	00	00	96	00
0x0FB290	00	00	00	00	00	00	00	00	00	01	00	00	96	00	00	00
0x0FB2A0	00	00	00	00	00	00	00	01	00	00	96	00	00	00	00	00
0x0FB2B0	00	00	00	00	00	01	00	00	96	00	00	00	00	00	00	00
0x0FB2C0	00	00	00	01	00	00	96	00	00	00	00	00	00	00	00	00
0x0FB2D0	00	01	00	00	96	00	00	00	00	00	00	00	00	00	00	01
0x0FB2E0	00	00	96	00	00	00	00	00	00	00	00	00	00	01	00	00
0x0FB2F0	96	00	00	00	00	00	00	00	00	00	00	01	00	00	96	00
0x0FB300	00	00	00	00	00	00	00	00	00	01	00	00	96	00	00	00
0x0FB310	00	00	00	00	00	00	00	01	00	00	96	00	00	00	00	00

Data Analysis

- But is it the vehicle speed log?
- Tracing the speed along to compare with the report. The 2-byte is 12 bytes apart. Find the first change in the speed, 58 8A

0x0FB4C0	00	00	00	00	00	00	00	00	00	00	01	00	00	96	00	00	00
0x0FB4D0	00	00	00	00	00	00	00	01	00	00	96	00	00	00	00	00	00
0x0FB4E0	00	00	00	00	00	00	01	00	00	96	00	00	00	00	00	00	00
0x0FB4F0	00	00	00	01	00	00	96	00	00	00	00	00	00	00	00	00	00
0x0FB500	00	01	00	00	96	00	00	00	00	00	00	00	00	00	00	00	01
0x0FB510	00	00	96	00	00	00	00	00	00	00	00	00	00	00	01	00	00
0x0FB520	96	00	00	00	00	00	00	00	00	01	00	00	96	00	00	00	00
0x0FB530	00	00	00	00	00	00	00	00	01	00	00	58	8A	00	00	00	00	x.....
0x0FB540	00	00	00	00	00	00	01	00	00	06	58	00	00	00	00	00	00x.....
0x0FB550	00	00	00	00	00	01	00	00	00	74	00	00	00	00	00	00	00t.....
0x0FB560	00	00	00	01	00	00	00	08	00	00	00	00	00	00	00	00	00
0x0FB570	00	01	00	00	00	01	00	00	00	00	00	00	00	00	00	01	00

Data Analysis: Confirmation

- Convert 58 8A to actual vehicle speed number:
- 58 8A to Decimal: 22,666
- Convert 22,666 to actual number:

$$22,666 / 256 = 88.54 \text{ mph} \sim 89 \text{ mph}$$

Record 1

Time (Seconds)	Vehicle Speed (mph)	Engine Speed (rpm)	Engine Load (%)	Throttle (%)	Brake Status	Clutch Status	Cruise Status	Lamp Status
-16	150	0	0.0	0.0	-	-	-	On
-15	150	0	0.0	0.0	-	-	-	On
-14	150	0	0.0	0.0	-	-	-	On
-13	150	0	0.0	0.0	-	-	-	On
-12	150	0	0.0	0.0	-	-	-	On
-11	150	0	0.0	0.0	-	-	-	On
-10	150	0	0.0	0.0	-	-	-	On
-9	150	0	0.0	0.0	-	-	-	On
-8	150	0	0.0	0.0	-	-	-	On
-7	150	0	0.0	0.0	-	-	-	On
-6	150	0	0.0	0.0	-	-	-	On
-5	150	0	0.0	0.0	-	-	-	On
-4	150	0	0.0	0.0	-	-	-	On
-3	150	0	0.0	0.0	-	-	-	On
-2	150	0	0.0	0.0	-	-	-	On
-1	150	0	0.0	0.0	-	-	-	On
0	150	0	0.0	0.0	-	-	-	On
1	89	0	0.0	0.0	-	-	-	On
2	6	0	0.0	0.0	-	-	-	On

Data Analysis

- What about engine RPM, load, throttle, etc.?
- The 14-byte block in Record 2 data, this has more than just 150 mph

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0x0FB950	00	00	00	02	14	F8	12	BD	00	00	00	00	00	00	00	00ø.½..... ^
0x0FB960	00	03	01	81	12	7C	00	00	00	00	00	00	00	00	00	02
0x0FB970	00	1B	12	BF	00	09	00	00	00	00	00	00	00	02	00	02	...¿.....
0x0FB980	11	3E	00	21	08	C4	00	00	00	00	02	00	00	11	42		.>.!..Ä.....B
0x0FB990	00	2C	29	03	00	00	00	00	00	02	00	5C	11	E7	00	3E	.,).....\..ç.>
0x0FB9A0	42	8E	00	00	00	00	00	02	02	7D	19	38	00	76	10	8F	B.....}.8.v..
0x0FB9B0	00	00	00	00	00	00	03	AB	15	37	00	3E	00	00	00	00«.7.>....
0x0FB9C0	00	00	00	00	04	0A	17	82	00	94	20	B5	00	00	00	00µ....
0x0FB9D0	00	00	04	C1	21	E3	00	A4	1F	7B	00	00	00	00	02		...Á!ă.▯ {.....
0x0FB9E0	05	96	1A	5C	00	00	00	00	00	00	00	00	00	02	05	E8	...\\.....è
0x0FB9F0	1A	40	00	81	0E	9D	00	00	00	00	00	00	06	72	21	77	.@.....r!w
0x0FBA00	00	B6	26	8D	00	00	00	00	00	00	07	BE	26	98	00	99	.¶&.....¾&...
0x0FBA10	17	84	00	00	00	00	00	00	08	75	28	36	00	20	00	00u(6. ..
0x0FBA20	00	00	00	00	00	02	08	6F	1D	BF	00	5B	00	00	00	00o ¿.[....
0x0FBA30	00	00	1E	FA	15	9B	78	6F	12	F7	01	D2	79	DC	00	00	.. ú..xo.÷.ÒyÛ..
0x0FBA40	96	00	00	00	00	00	00	00	00	00	00	01	00	00	96	00
0x0FBA50	00	00	00	00	00	00	00	00	00	01	00	00	96	00	00	00

Data Analysis: Result

Byte	3 & 4	5 & 6	7 & 8	9 & 10
Hex	07 BE	26 98	00 99	17 84
Convert to Decimal	1,982	9,880	153	6020
Resolution	1/256 mph/bit	1/8 RPM/bit	1/4 %/bit	1/256 %/bit
Actual Number	7.74 mph	1,235 RPM	38.25%	23.52%
	Vehicle Speed	Engine Speed	Throttle	Engine Load

Record 2

Time (Seconds)	Vehicle Speed (mph)	Engine Speed (rpm)	Engine Load (%)	Throttle (%)	Brake Status	Clutch Status	Cruise Status	Lamp Status
11	6	840	14.6	32.3	-	On	-	-
12	6	1071	38.6	45.5	-	-	-	-
13	8	1235	23.5	38.3	-	-	-	-
14	8	1287	0.0	8.0	-	-	-	-
15	8	952	0.0	22.8	-	On	-	-

Data Analysis: Alternative Approach

Another approach to locate sudden deceleration data in binary file:

- Log CAN traffic when downloading sudden deceleration report with Cummins PowerSpec
- Compare the log file with binary to find the pattern.

Tools

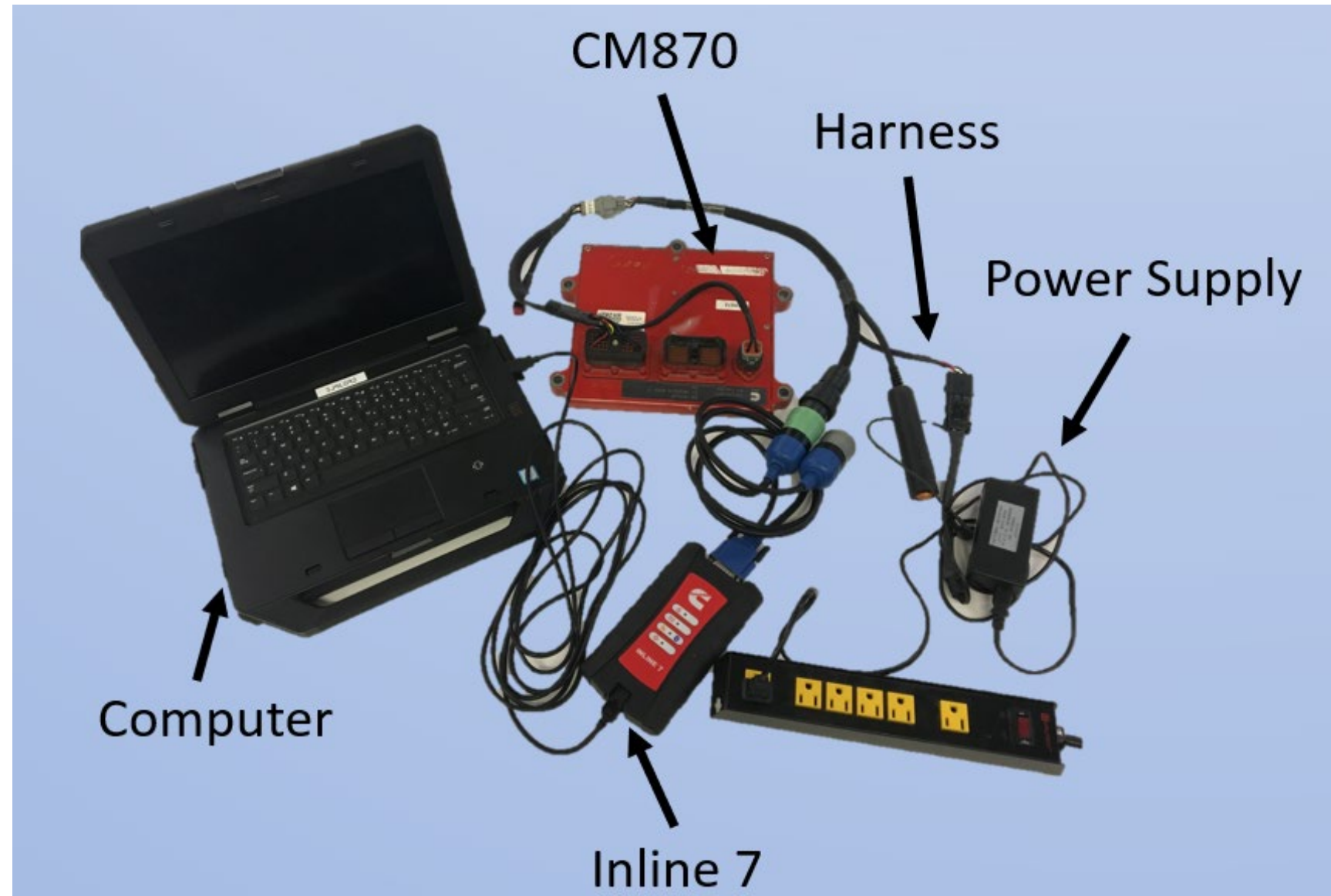


Photo from
<https://www.diesellaptops.com/collections/cummins/products/cummins-inline-7-data-link-adapter>



Connecting Harness

Setup



NMFTA CAN Logger

National Motor Freight Traffic Association and National Science Foundation CAN Data Collection Project

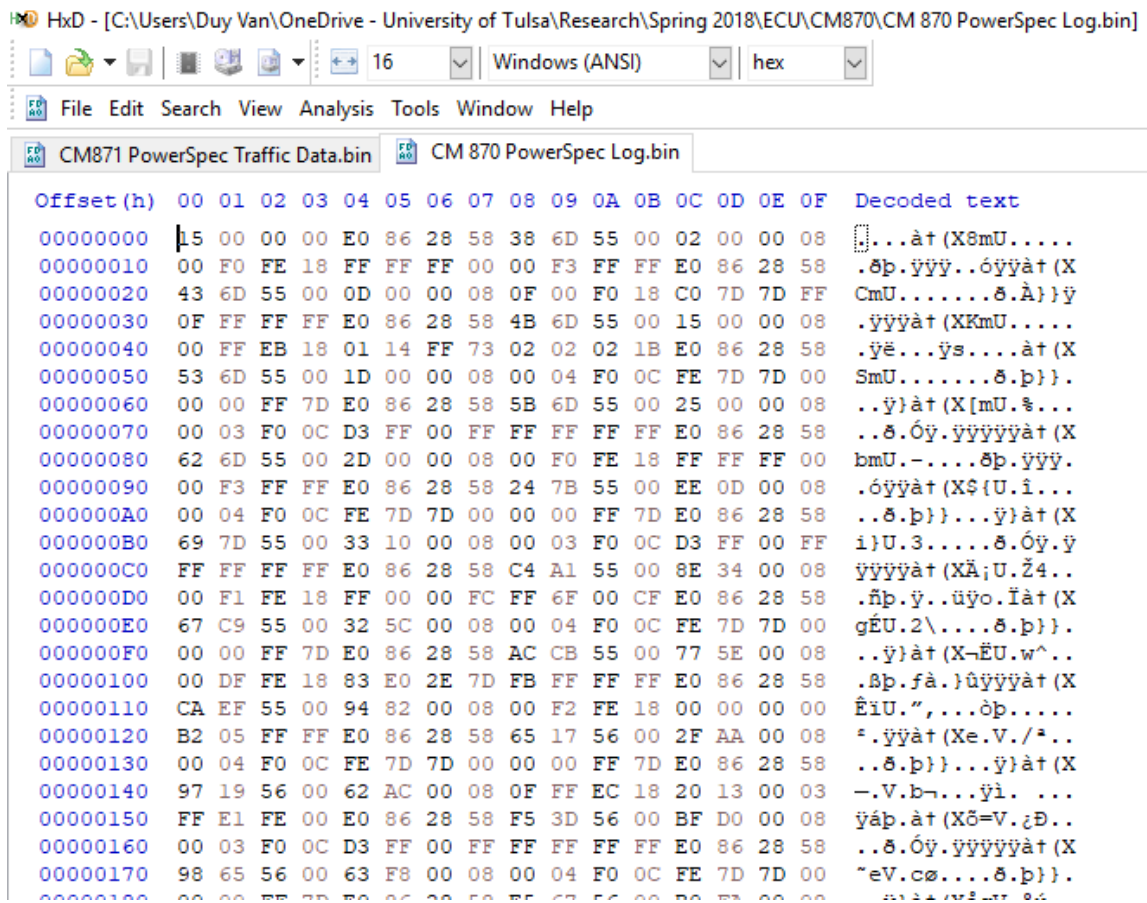


Open Source at:

<https://www.github.com/SystemsCyber/CAN-Logger-3/>

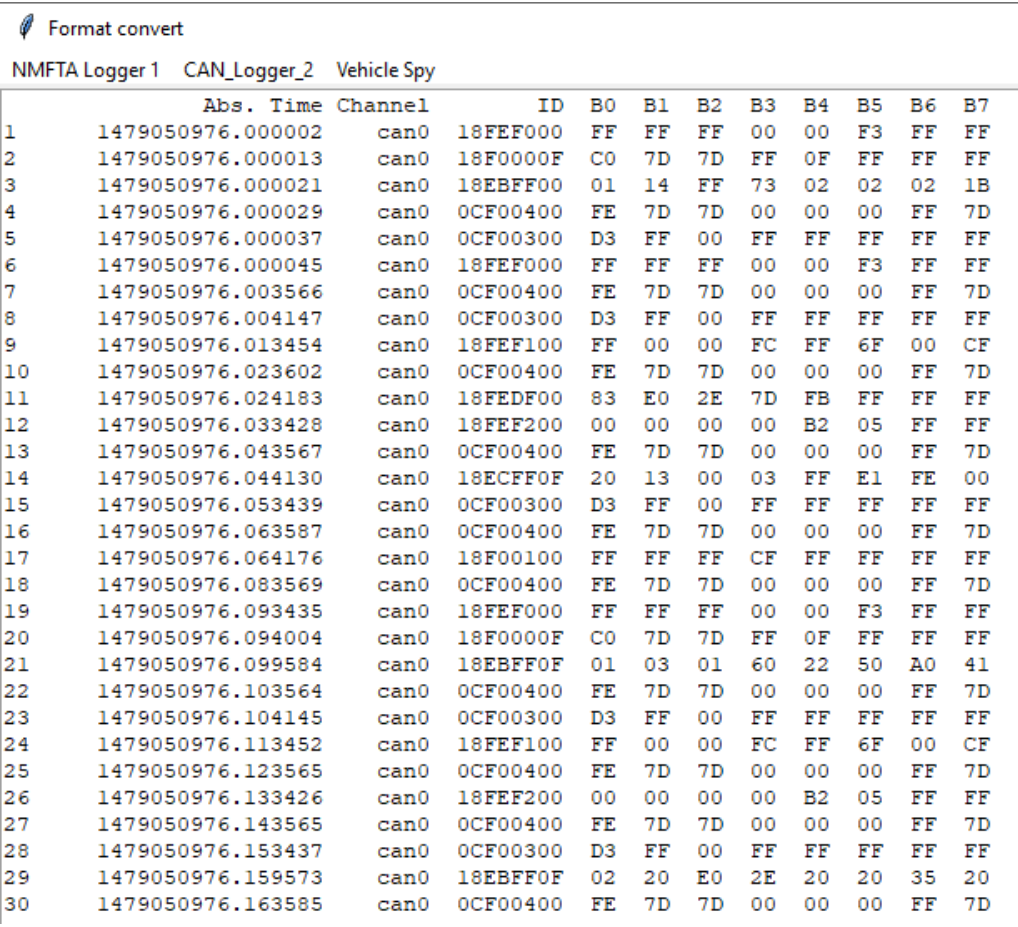
Downloading Data

CAN traffic was also logged while downloading



The screenshot shows the HxD hex editor interface. The title bar indicates the file path: C:\Users\Duy Van\OneDrive - University of Tulsa\Research\Spring 2018\ECU\CM870\CM 870 PowerSpec Log.bin. The menu bar includes File, Edit, Search, View, Analysis, Tools, Window, and Help. The toolbar shows various file operations and a hex/ASCII toggle. The main window displays two tabs: 'CM871 PowerSpec Traffic Data.bin' and 'CM 870 PowerSpec Log.bin'. The active tab shows a hex dump with offset (h) from 00 to 0F and decoded text. The decoded text is garbled, likely due to incorrect encoding or a corrupted file.

CAN traffic logged in raw format



The screenshot shows the NMFTA Logger 1 interface. The title bar includes 'Format convert'. The menu bar includes NMFTA Logger 1, CAN_Logger_2, and Vehicle Spy. The main window displays a table of CAN traffic data in a readable format.

	Abs. Time	Channel	ID	B0	B1	B2	B3	B4	B5	B6	B7
1	1479050976.000002	can0	18FEF000	FF	FF	FF	00	00	F3	FF	FF
2	1479050976.000013	can0	18F0000F	C0	7D	7D	FF	0F	FF	FF	FF
3	1479050976.000021	can0	18EBFF00	01	14	FF	73	02	02	02	1B
4	1479050976.000029	can0	0CF00400	FE	7D	7D	00	00	00	FF	7D
5	1479050976.000037	can0	0CF00300	D3	FF	00	FF	FF	FF	FF	FF
6	1479050976.000045	can0	18FEF000	FF	FF	FF	00	00	F3	FF	FF
7	1479050976.003566	can0	0CF00400	FE	7D	7D	00	00	00	FF	7D
8	1479050976.004147	can0	0CF00300	D3	FF	00	FF	FF	FF	FF	FF
9	1479050976.013454	can0	18FEF100	FF	00	00	FC	FF	6F	00	CF
10	1479050976.023602	can0	0CF00400	FE	7D	7D	00	00	00	FF	7D
11	1479050976.024183	can0	18FEDF00	83	E0	2E	7D	FB	FF	FF	FF
12	1479050976.033428	can0	18FEF200	00	00	00	00	B2	05	FF	FF
13	1479050976.043567	can0	0CF00400	FE	7D	7D	00	00	00	FF	7D
14	1479050976.044130	can0	18ECFF0F	20	13	00	03	FF	E1	FE	00
15	1479050976.053439	can0	0CF00300	D3	FF	00	FF	FF	FF	FF	FF
16	1479050976.063587	can0	0CF00400	FE	7D	7D	00	00	00	FF	7D
17	1479050976.064176	can0	18F00100	FF	FF	FF	CF	FF	FF	FF	FF
18	1479050976.083569	can0	0CF00400	FE	7D	7D	00	00	00	FF	7D
19	1479050976.093435	can0	18FEF000	FF	FF	FF	00	00	F3	FF	FF
20	1479050976.094004	can0	18F0000F	C0	7D	7D	FF	0F	FF	FF	FF
21	1479050976.099584	can0	18EBFF0F	01	03	01	60	22	50	A0	41
22	1479050976.103564	can0	0CF00400	FE	7D	7D	00	00	00	FF	7D
23	1479050976.104145	can0	0CF00300	D3	FF	00	FF	FF	FF	FF	FF
24	1479050976.113452	can0	18FEF100	FF	00	00	FC	FF	6F	00	CF
25	1479050976.123565	can0	0CF00400	FE	7D	7D	00	00	00	FF	7D
26	1479050976.133426	can0	18FEF200	00	00	00	00	B2	05	FF	FF
27	1479050976.143565	can0	0CF00400	FE	7D	7D	00	00	00	FF	7D
28	1479050976.153437	can0	0CF00300	D3	FF	00	FF	FF	FF	FF	FF
29	1479050976.159573	can0	18EBFF0F	02	20	E0	2E	20	20	35	20
30	1479050976.163585	can0	0CF00400	FE	7D	7D	00	00	00	FF	7D

CAN traffic logged in readable format

CAN Data Logging Results

There is pattern for the Sudden Deceleration records

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B
000F31BC	00	00	00	00	00	00	00	00	00	00	00	00
000F31C8	00	00	00	00	00	00	00	00	00	00	00	00
000F31D4	00	00	00	00	0C	31	00	00	00	00	00	00
000F31E0	00	00	00	73	00	02	1E	FA	15	9B	85	8A
000F31EC	12	F6	01	D2	79	DC	00	00	96	00	00	00
000F31F8	00	00	00	00	00	00	00	01	00	00	96	00
000F3204	00	00	00	00	00	00	00	00	00	01	00	00
000F3210	96	00	00	00	00	00	00	00	00	00	00	01
000F321C	00	00	96	00	00	00	00	00	00	00	00	00
000F3228	00	01	00	00	96	00	00	00	00	00	00	00
000F3234	00	00	00	01	00	00	96	00	00	00	00	00
000F3240	00	00	00	00	00	01	00	00	96	00	00	00
000F324C	00	00	00	00	00	00	00	01	00	00	96	00

Raw binary data from KTAG extraction

1479051111.967139	can0	18EBFF00	08	04	AF	00	03	03	6C	00
1479051111.976171	can0	18EBFA00	01	45	1A	A0	00	00	04	26
1479051111.986092	can0	18EBFA00	02	1E	FA	15	9B	85	8A	12
1479051111.996095	can0	18EBFA00	03	F6	01	D2	79	DC	00	00
1479051112.006143	can0	18EBFA00	04	96	00	00	00	00	00	00
1479051112.016150	can0	18EBFA00	05	00	00	00	00	01	00	00
1479051112.026145	can0	18EBFA00	06	96	00	00	00	00	00	00
1479051112.026713	can0	18EBFF00	09	04	01	66	00	04	01	94
1479051112.036134	can0	18EBFA00	07	00	00	00	00	01	00	00
1479051112.046148	can0	18EBFA00	08	96	00	00	00	00	00	00
1479051112.056151	can0	18EBFA00	09	00	00	00	00	01	00	00
1479051112.066164	can0	18EBFA00	0A	96	00	00	00	00	00	00
1479051112.076132	can0	18EBFA00	0B	00	00	00	00	01	00	00
1479051112.086140	can0	18EBFA00	0C	96	00	00	00	00	00	00
1479051112.086713	can0	18EBFF00	0A	04	03	01	B9	04	04	03
1479051112.096128	can0	18EBFA00	0D	00	00	00	00	01	00	00
1479051112.106137	can0	18EBFA00	0E	96	00	00	00	00	00	00
1479051112.116171	can0	18EBFA00	0F	00	00	00	00	01	00	00

Logged CAN traffic data, filtered for J1939 Transport Protocol messages

Interpreter Python Source Code Snippet

Attribution Data

```
with open(filename,'rb') as binfile:
    raw_data = binfile.read()

#Extract run time, occurrence distance, and temp of 3 records
ECM_run_time1 = struct.unpack(">L",raw_data[record1:record1+4])[0]/4
Occurrence_distance1 = struct.unpack(">L",raw_data[record1+20:record1+24])[0]/205.99605
Temp1 = (((((struct.unpack(">L",raw_data[record1+18:record1+22])[0]) & 0xFFFF0000 )>> 16)/128)*9/5)+32

ECM_run_time2 = struct.unpack(">L",raw_data[record2:record2+4])[0]/4
Occurrence_distance2 = struct.unpack(">L",raw_data[record2+20:record2+24])[0]/205.99605
Temp2 = (((((struct.unpack(">L",raw_data[record2+18:record2+22])[0]) & 0xFFFF0000 )>> 16)/128)*9/5)+32

ECM_run_time3 = struct.unpack(">L",raw_data[record3:record3+4])[0]/4
Occurrence_distance3 = struct.unpack(">L",raw_data[record3+20:record3+24])[0]/205.99605
Temp3 = (((((struct.unpack(">L",raw_data[record3+18:record3+22])[0]) & 0xFFFF0000 )>> 16)/128)*9/5)+32
```


Attribution Result

Record 1 ECM occurrence run time (s): 10437516.0

Record 1 ECM occurrence distance (mile): 109323.35838478456

Record 1 ECM occurrence air temperature (F): 71.9234375

Record 2 ECM occurrence run time (s): 29454947.0

Record 2 ECM occurrence distance (mile): 250785.41069112733

Record 2 ECM occurrence air temperature (F): 55.3015625

Record 3 ECM occurrence run time (s): 6186154.0

Record 3 ECM occurrence distance (mile): 66872.23371516104

Record 3 ECM occurrence air temperature (F): 117.359375

Python Code for Sudden Decel Records

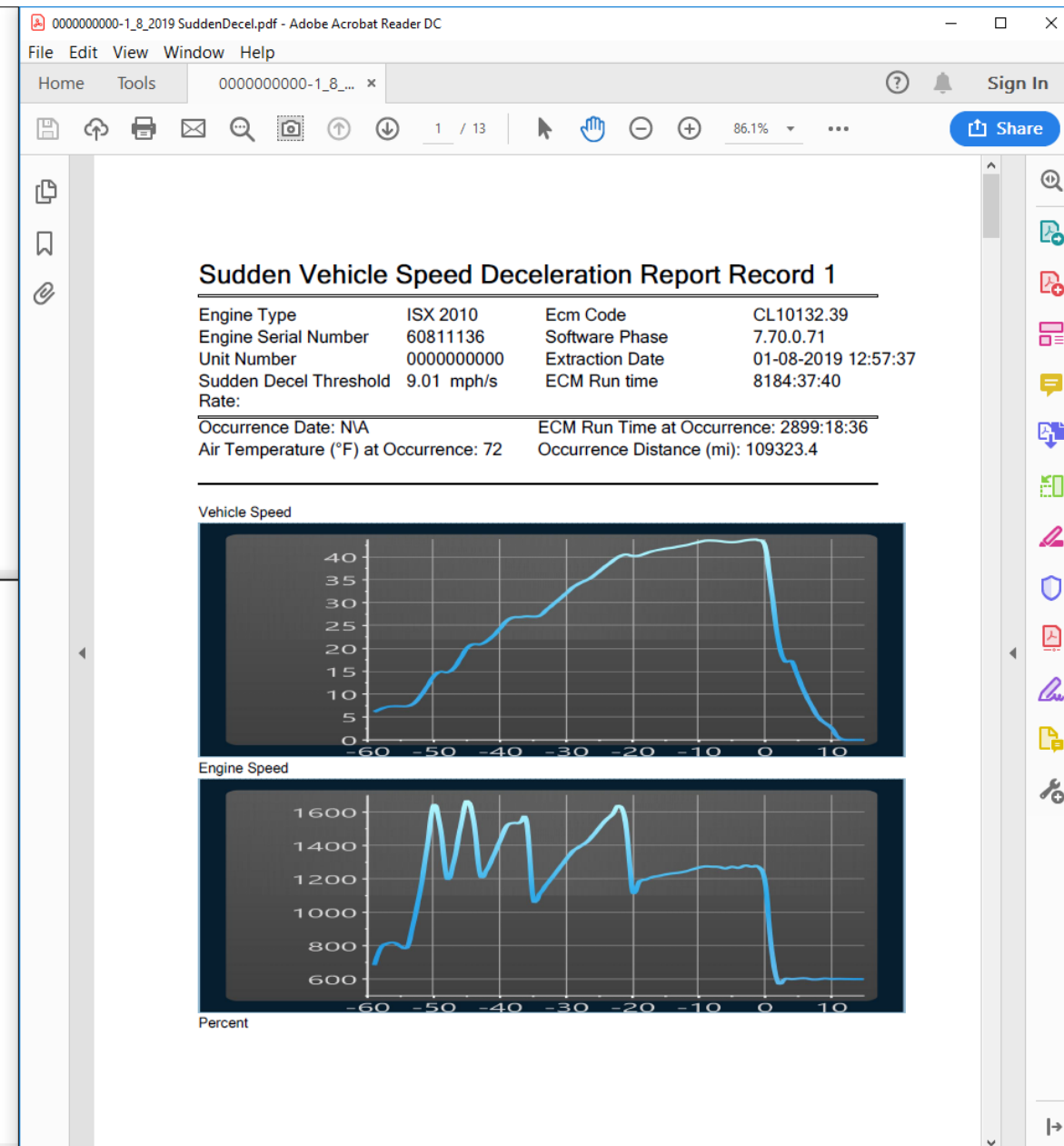
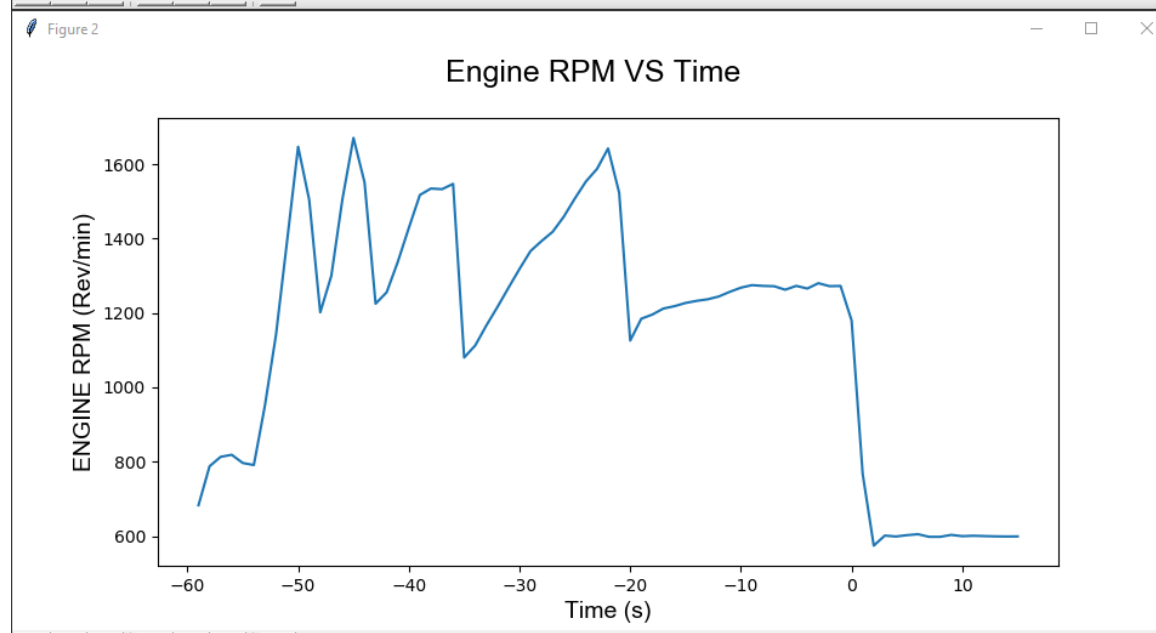
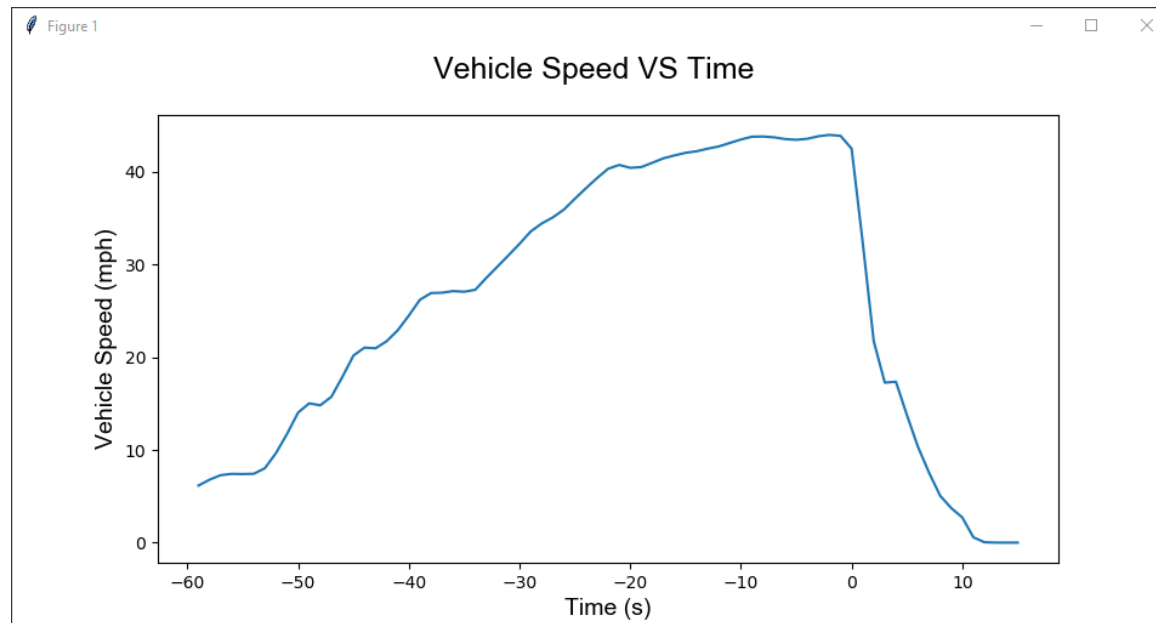
```
#Parsing through the raw data
for i in range(int((record_size-header_size)/block_size)):
    speed1 = ((struct.unpack(">L",raw_data[record1+24+i*block_size : record1+28+i*block_size])[0]) & 0x0000FFFF )/102.455
    rpm1 = ((struct.unpack(">L",raw_data[record1+28+i*block_size : record1+32+i*block_size])[0]) & 0x0000FFFF )/8

    speed2 = ((struct.unpack(">L",raw_data[record2+24+i*block_size : record2+28+i*block_size])[0]) & 0x0000FFFF )/102.455
    rpm2 = ((struct.unpack(">L",raw_data[record2+28+i*block_size : record2+32+i*block_size])[0]) & 0x0000FFFF )/8

    speed3 = ((struct.unpack(">L",raw_data[record3+24+i*block_size : record3+28+i*block_size])[0]) & 0x0000FFFF )/102.455
    rpm3 = ((struct.unpack(">L",raw_data[record3+28+i*block_size : record3+32+i*block_size])[0]) & 0x0000FFFF )/8

    time = -59+i
```

Graphical Result From Binary Interpretation



Data Analysis: Missing Data

- Reverse Engineered only 8 bytes in the 14 byte block.
 - What do other bytes mean?
 - Which one is the brake status, clutch status, etc.?

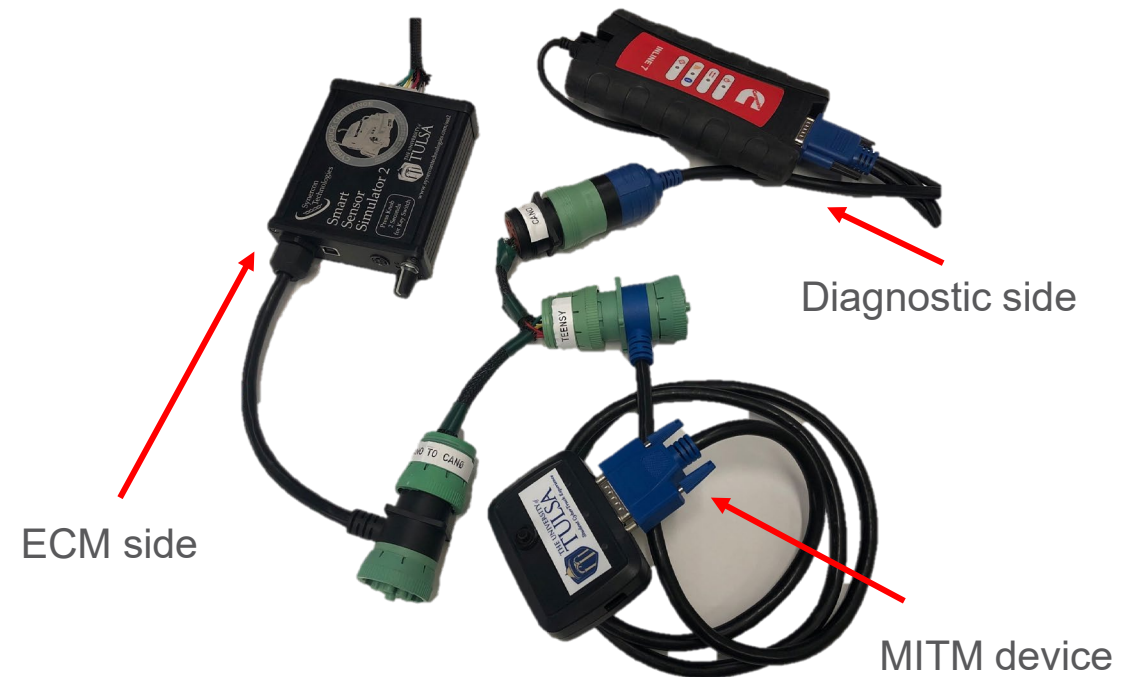
Record 2

Time (Seconds)	Vehicle Speed (mph)	Engine Speed (rpm)	Engine Load (%)	Throttle (%)	Brake Status	Clutch Status	Cruise Status	Lamp Status
11	6	840	14.6	32.3	-	On	-	-
12	6	1071	38.6	45.5	-	-	-	-
13	8	1235	23.5	38.3	-	-	-	-
14	8	1287	0.0	8.0	-	-	-	-
15	8	952	0.0	22.8	-	On	-	-



Man In The Middle Attack

- Man In The Middle (MITM) attack for reverse engineering
 - Sudden deceleration data sent from the ECM will be modified by the MITM device to observe how the it changes the record



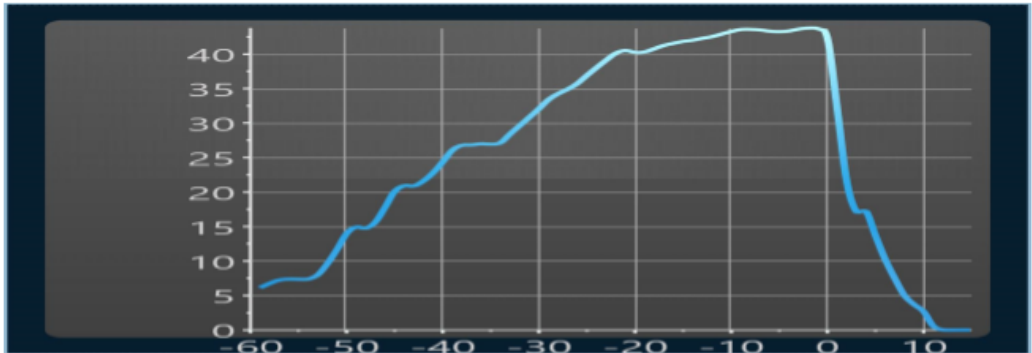
Machine-In-the-Middle (MITM) Attack

Sudden Vehicle Speed Deceleration Report Record 1

Engine Type	ISX 2010	Ecm Code	CL10132.39
Engine Serial Number	60811136	Software Phase	7.70.0.71
Unit Number	0000000000	Extraction Date	04-03-2019 04:37:51
Sudden Decel Threshold Rate:	N/A	ECM Run time	8227:56:32

Occurrence Date: N/A ECM Run Time at Occurrence: 2899:18:36
Air Temperature (°F) at Occurrence: 72 Occurrence Distance (mi): 109323.4

Vehicle Speed



Record 1

Time (Seconds)	Vehicle Speed (mph)	Engine Speed (rpm)	Engine Load (%)	Throttle (%)	Brake Status	Clutch Status	Cruise Status	Lamp Status
-59	6	683	34.8	30.1	-	-	-	-
-58	7	788	33.6	32.2	-	-	-	-
-57	7	813	21.9	27.5	-	-	-	-

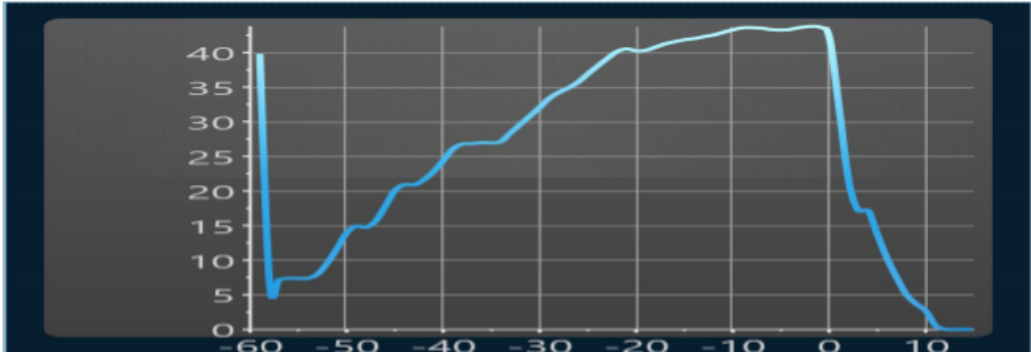
Genuine Data

Sudden Vehicle Speed Deceleration Report Record 1

Engine Type	ISX 2010	Ecm Code	CL10132.39
Engine Serial Number	60811136	Software Phase	7.70.0.71
Unit Number	0000000000	Extraction Date	04-03-2019 02:08:09
Sudden Decel Threshold Rate:	N/A	ECM Run time	8225:27:34

Occurrence Date: N/A ECM Run Time at Occurrence: 2899:18:36
Air Temperature (°F) at Occurrence: 72 Occurrence Distance (mi): 109323.4

Vehicle Speed

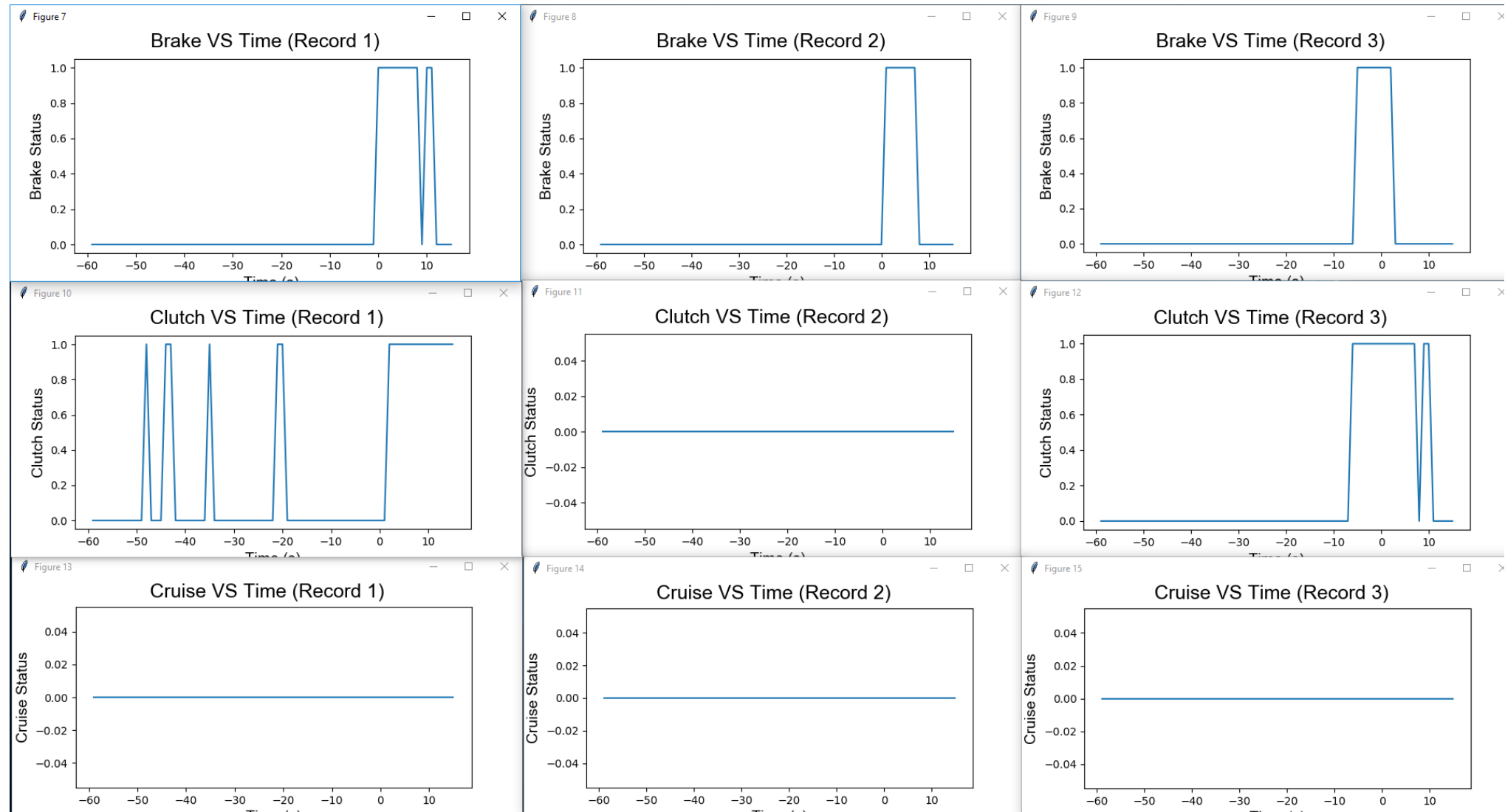


Record 1

Time (Seconds)	Vehicle Speed (mph)	Engine Speed (rpm)	Engine Load (%)	Throttle (%)	Brake Status	Clutch Status	Cruise Status	Lamp Status
-59	40	683	34.8	30.1	-	-	-	-
-58	7	788	33.6	32.2	-	-	-	-
-57	7	813	21.9	27.5	-	-	-	-

Attack Data

Brake, Clutch, Cruise Results





Data Manipulation

Forensic Soundness and Protecting Against

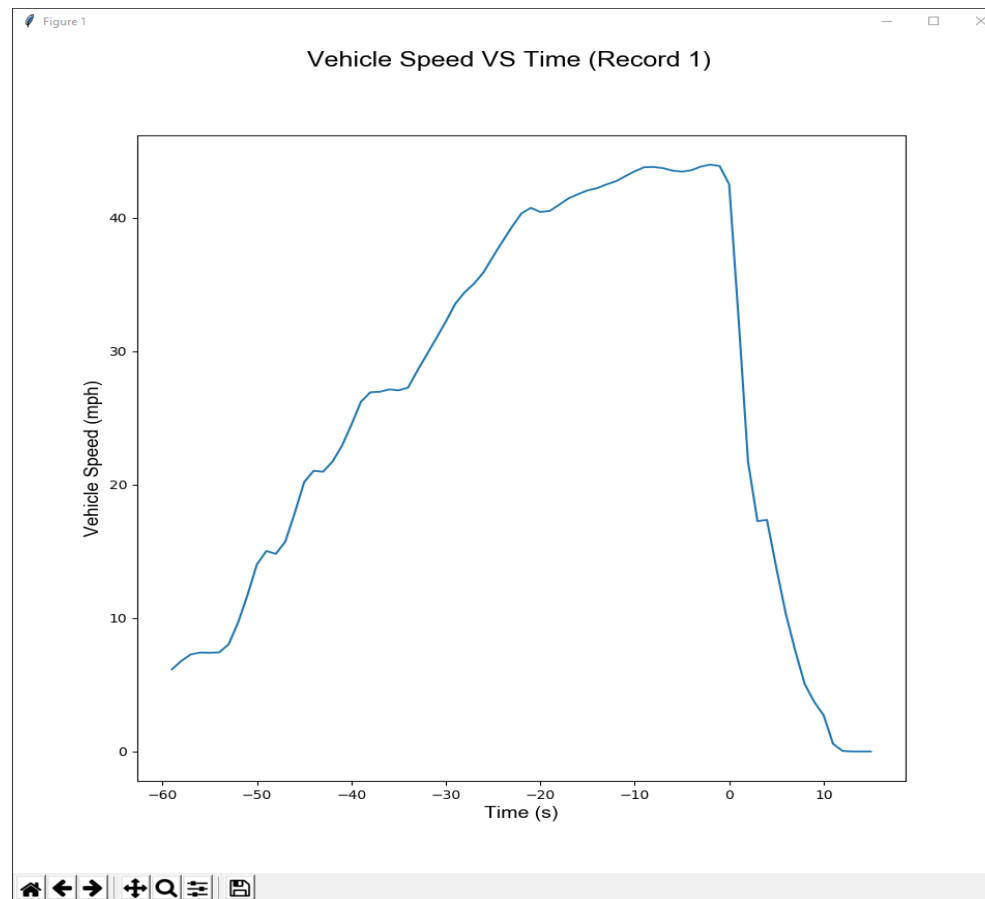
Editing Data in Hex

HxD - [C:\Users\dailyadmin\OneDrive - University of Tulsa\Research\Summer 2019\Florida Trip\back up - attacked.MPC]

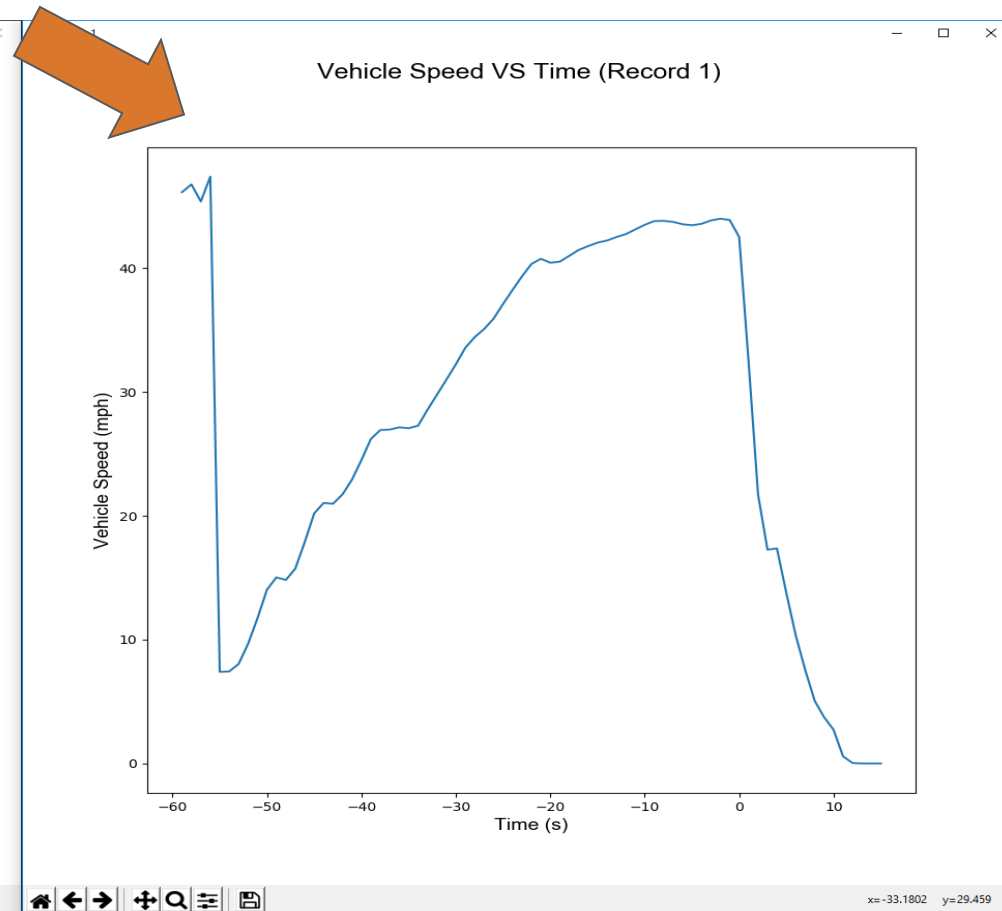
	File Edit Search View Analysis Tools Window Help																
	16 Windows (ANSI) hex																
back up - attacked.MPC																	
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00009510	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00009520	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00009530	1B	EB	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.ë.....
00009540	00	FF	FF	FF	02	7D	0E	30	FF	FF	FF	FF	01	00	00	01	.ÿÿÿ.}.0ÿÿÿÿ....
00009550	01	01	01	00	01	01	0B	17	01	57	A1	74	00	00	13	77W;t...w
00009560	00	00	15	58	00	00	1E	15	22	C4	00	00	00	00	13	B3	...X...."Ä....,
00009570	00	00	18	9F	00	00	20	35	21	98	00	00	00	00	13	2A	...ÿ.. 5!~....*
00009580	00	00	19	69	00	00	1B	76	15	E0	00	00	00	00	13	F3	...i...v.à....ø
00009590	00	00	19	96	00	00	16	0D	0A	8C	00	00	00	00	02	F6	...-.....Œ.....ö
000095A0	00	00	18	E5	00	00	0F	B9	00	00	00	00	00	00	02	F9	...å...¹.....ù
000095B0	00	00	18	B9	00	00	1D	EC	1A	90	00	00	00	00	03	37	...¹....ì.....7
000095C0	00	00	1D	B7	00	00	2C	7D	30	0C	00	00	00	00	03	DE	...·... , } 0.....Ð
000095D0	00	00	23	A9	00	00	33	0C	27	10	00	00	00	00	04	B2	..#©..3.'.....²
000095E0	00	00	2B	85	00	00	3F	23	30	70	00	00	00	00	05	9E	..+....?#0p.....ž
000095F0	00	00	33	76	00	00	40	94	2B	5C	00	00	00	00	06	04	..3v..@"+\.....
00009600	00	00	2F	02	00	00	00	8E	00	00	00	00	00	00	05	EE	../.....Ž.....î
00009610	00	00	25	8D	00	01	13	FB	00	00	00	00	00	00	06	4C	..%.....û.....L

Manipulating Speed Records

Original Authentic Record



Manipulated Record



Forensic Soundness

- **Meaning** is a term that denotes confidence in the interpretation of extracted evidence data.
- **Error Detection** denotes processes for detecting or predicting errors in the forensic process.
- **Transparency** means the forensic process is documented, known, and verifiable.
- **Expertise** is required for investigators examining digital data.
- **Tampering detection** involves processes to evaluate if this has occurred.

Forensic Soundness: Applied

Tamper Detection

Digitally sign the file with a secure hash algorithm

Goal: Verify mathematically the data has not been changed from its original form.

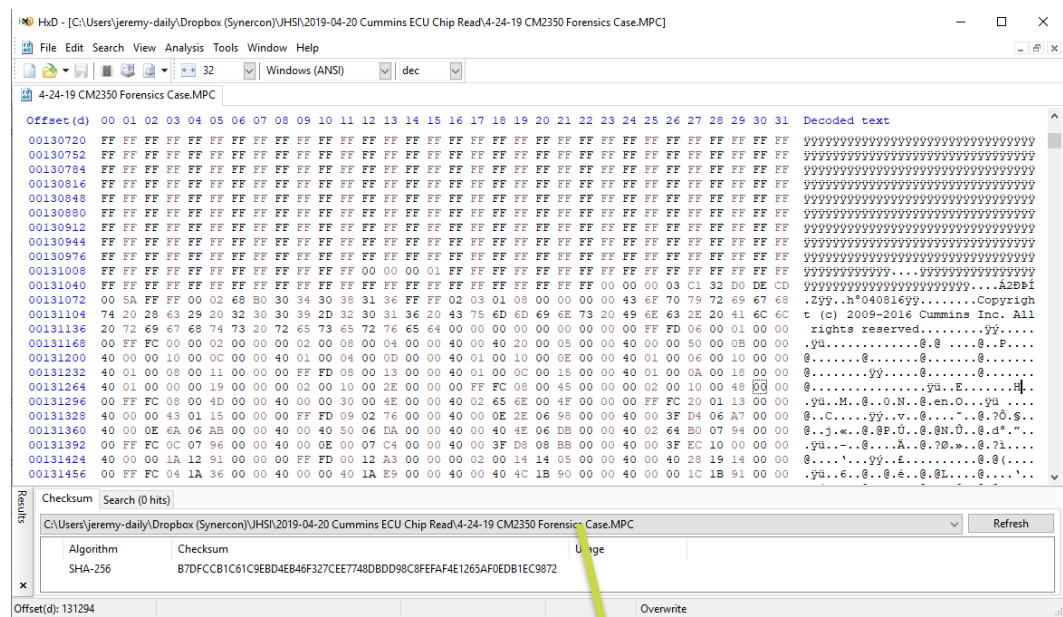
Calculated hash values match each time file is used

Challenge: How to compute the original hash?

Cryptographic Hashing

- Secure Hash Algorithm (SHA-256)
 - Calculates a unique 256-bit number based on file contents
 - File contents cannot be determined from the hash
 - Unique for each file (i.e. little chance of a “collision”)
- Windows right click utilities:
 - https://www.nirsoft.net/utils/hash_my_files.html
 - <https://www.tenforums.com/tutorials/78681-add-file-hash-context-menu-windows-8-10-a.html>

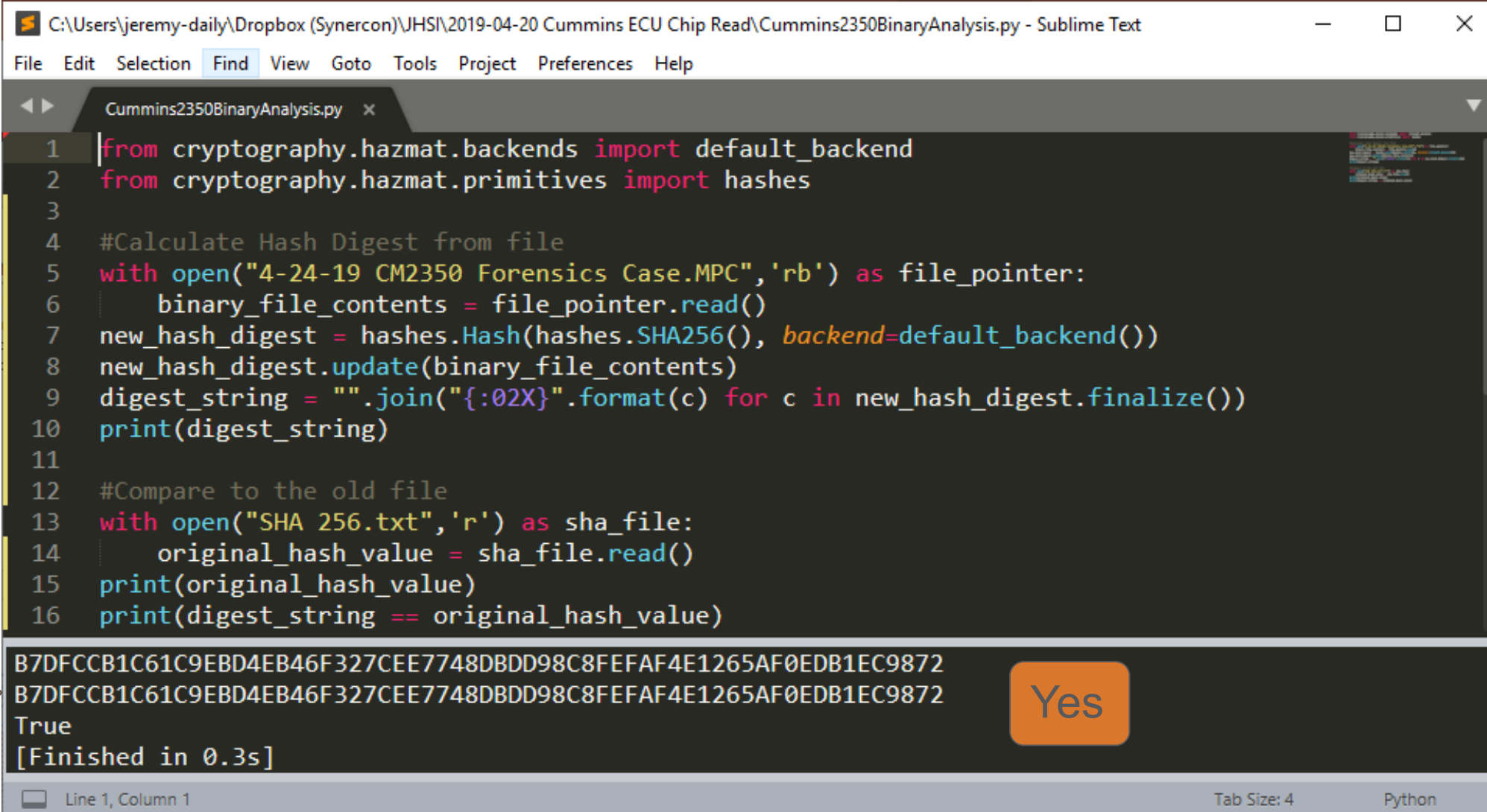
Calculate Hash with Hex Editor Utility



C:\Users\jeremy-daily\Dropbox (Synercon)\JHSI\2019-04-20 Cummins ECU Chip Read\4-24-19 CM2350 Forensics Case.MPC

Algorithm	Checksum
SHA-256	B7DFCCB1C61C9EBD4EB46F327CEE7748DBDD98C8FEFAF4E1265AF0EDB1EC9872
Offset(d): 131294	

Python Source Code: Do the hashes match?



```
C:\Users\jeremy-daily\Dropbox (Synercon)\JHSI\2019-04-20 Cummins ECU Chip Read\Cummins2350BinaryAnalysis.py - Sublime Text
File Edit Selection Find View Goto Tools Project Preferences Help

Cummins2350BinaryAnalysis.py x
1 from cryptography.hazmat.backends import default_backend
2 from cryptography.hazmat.primitives import hashes
3
4 #Calculate Hash Digest from file
5 with open("4-24-19 CM2350 Forensics Case.MPC",'rb') as file_pointer:
6     binary_file_contents = file_pointer.read()
7 new_hash_digest = hashes.Hash(hashes.SHA256(), backend=default_backend())
8 new_hash_digest.update(binary_file_contents)
9 digest_string = "".join("{:02X}".format(c) for c in new_hash_digest.finalize())
10 print(digest_string)
11
12 #Compare to the old file
13 with open("SHA 256.txt",'r') as sha_file:
14     original_hash_value = sha_file.read()
15 print(original_hash_value)
16 print(digest_string == original_hash_value)

B7DFCCB1C61C9EBD4EB46F327CEE7748DBDD98C8FEFAF4E1265AF0EDB1EC9872
B7DFCCB1C61C9EBD4EB46F327CEE7748DBDD98C8FEFAF4E1265AF0EDB1EC9872
True
[Finished in 0.3s]
```

Yes

Line 1, Column 1 Tab Size: 4 Python

Hash Values Do Not Match

New folder

FileHomeShareView

StudentAdmin > OneDrive - University of Tulsa > Research > Summer 2019 > Florida Trip > New folder

Quick access

Desktop

Downloads

Documents

Pictures

6-3-2019 Red CM23

Florida Trip

Red Cm2250

Silver CM2350

OneDrive - University

Research

This PC

3D Objects

Desktop

Name	Status	Date modified	Type	Size
back up - attaccked.MPC	✓	6/3/2019 3:42 PM	MPC File	3,073 KB
back up.MPC	✓	1/8/2019 2:21 PM	MPC File	3,073 KB

Checksum information

Name: back up - attaccked.MPC
Size: 3146752 bytes (3 MB)

SHA256:
771F7B49544EC6426D156FF1B5882130214CDFF2AD32F4C48D3BBEEB2B
F7878A

OK

Checksum information

Name: back up.MPC
Size: 3146752 bytes (3 MB)

SHA256:
F4E46ED2626C3E85FABC66146757FB1084E92412860BC9470EE57499A21
B433F

OK



Recommended Practice



Recommended Practice

Take photos or video of opening the ECU.

Document video creation time.

Created at 9:09

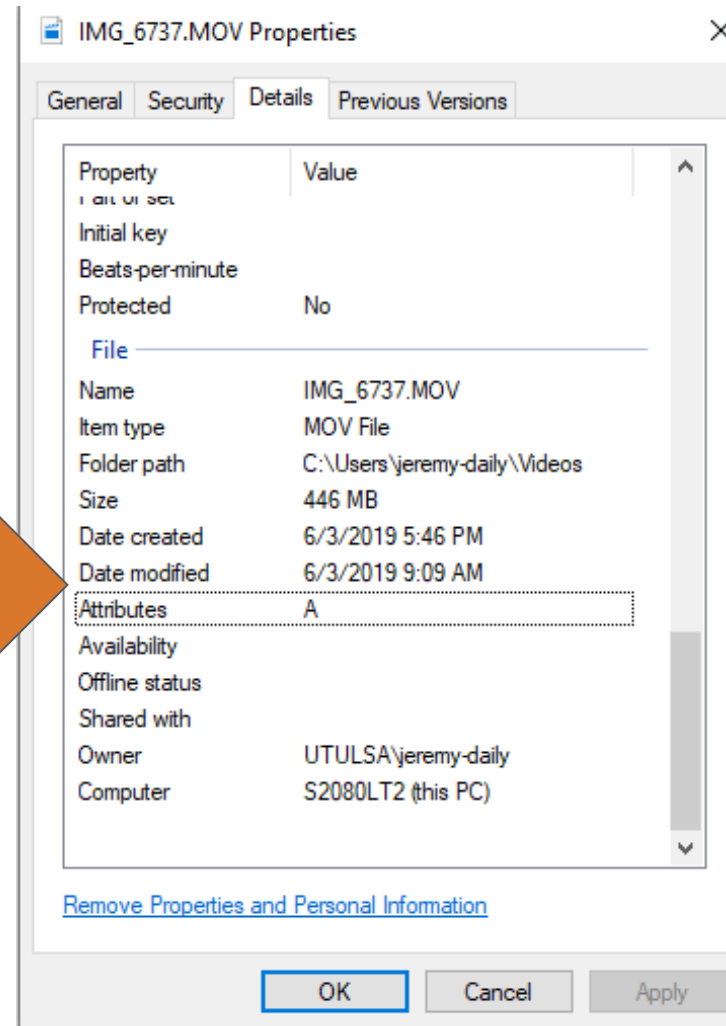


Image the ECU



Hash the data after Extraction

K-TAG

KTAG

Programming

6-3-2019 Red CM2350

File Home Share View

StudentAdmin > OneDrive - University of Tulsa > Research > Summer 2019 > Florida Trip > 6-3-2019 Red CM2350

<input type="checkbox"/>	Name	Status	Date modified	Type	Size
<input type="checkbox"/>	red CM2350 6-3-2019	✓	6/3/2019 9:10 AM	File	1,801 KB
<input checked="" type="checkbox"/>	red CM2350 6-3-2019.MPC	✓	6/3/2019 9:10 AM	MPC File	4,128 KB

Quick access

Desktop

Downloads

Documents

Pictures

Florida Trip

Red Cm2250

Red CM2350

Silver CM2350

OneDrive - University

Research

This PC

Checksum information

Name: red CM2350 6-3-2019.MPC

Size: 4227072 bytes (4 MB)

SHA256:

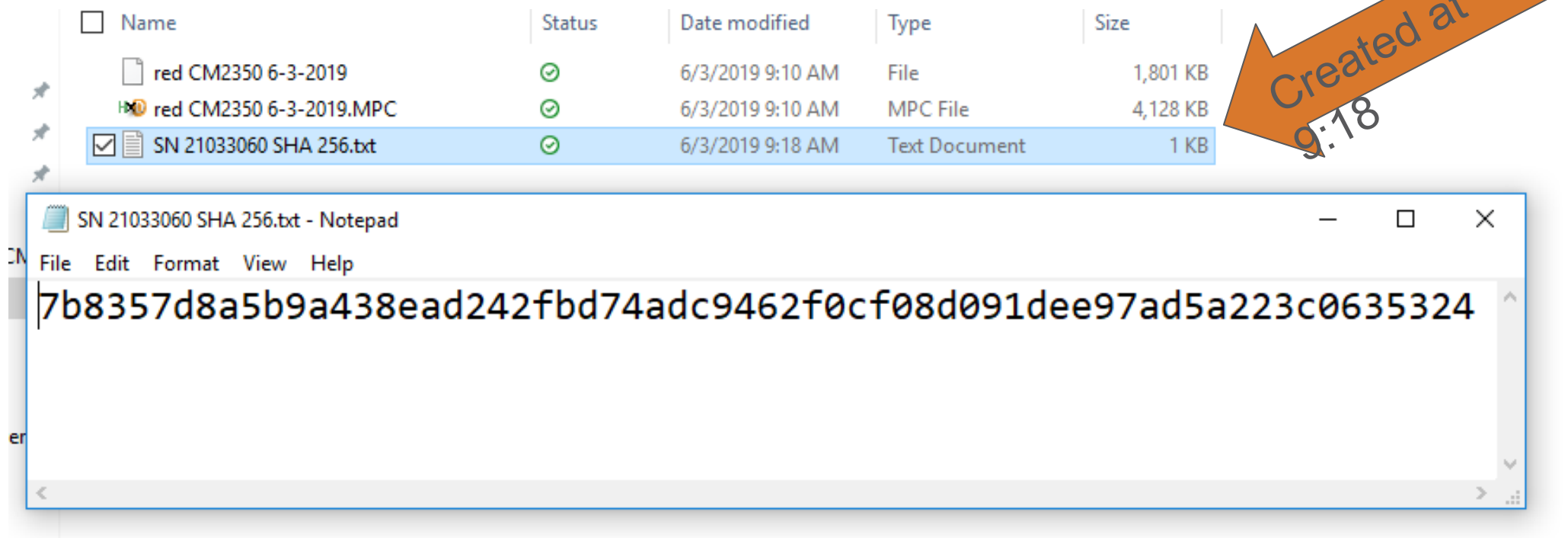
7B8357D8A5B9A438EAD242FBD74ADC9462F0CF08D091DEE97AD5A223C0635324

OK

Recommended Practice

Immediately after imaging the chip memory:

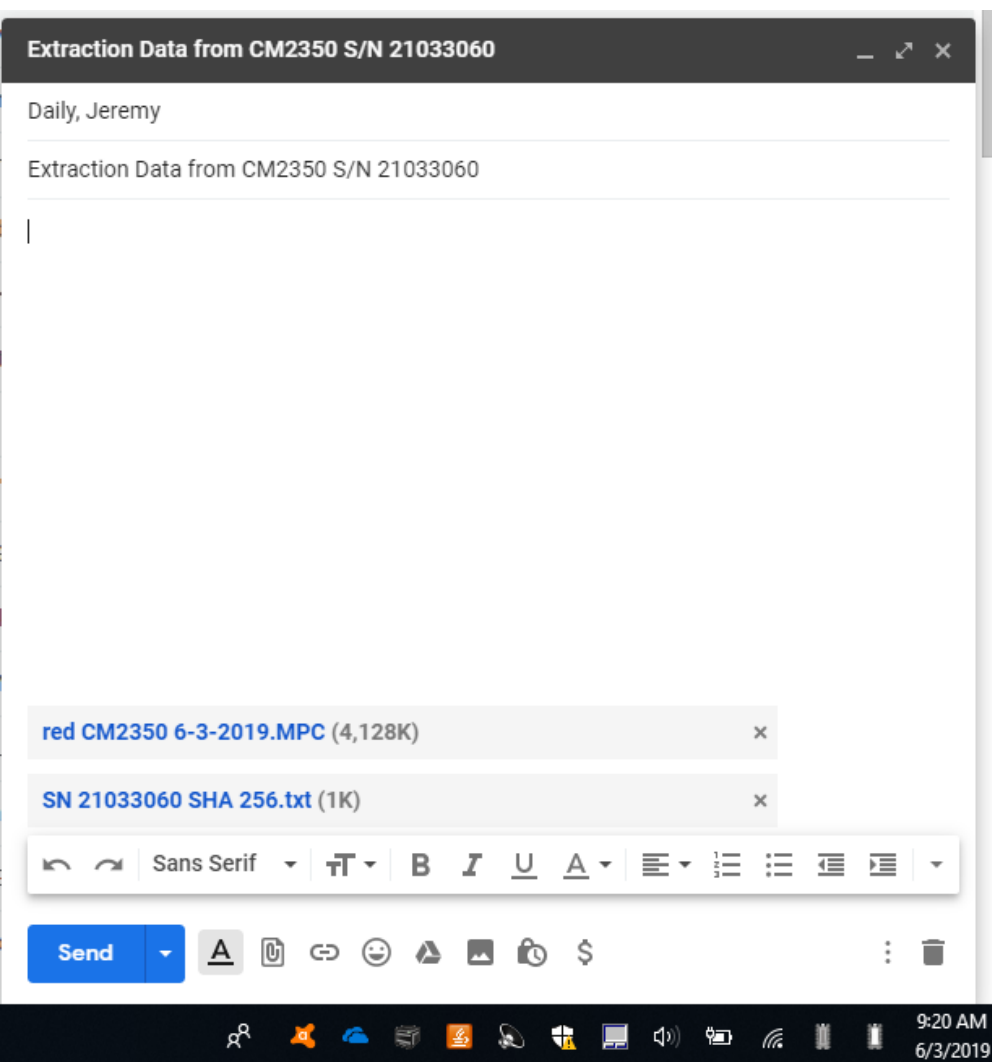
- Calculate the SHA-256 and save it as a text file.



Recommended Practice

E-Mail the SHA-256 digest value to a trusted party

Establishes a record with a timestamp when the SHA was calculated



Daily, Jeremy

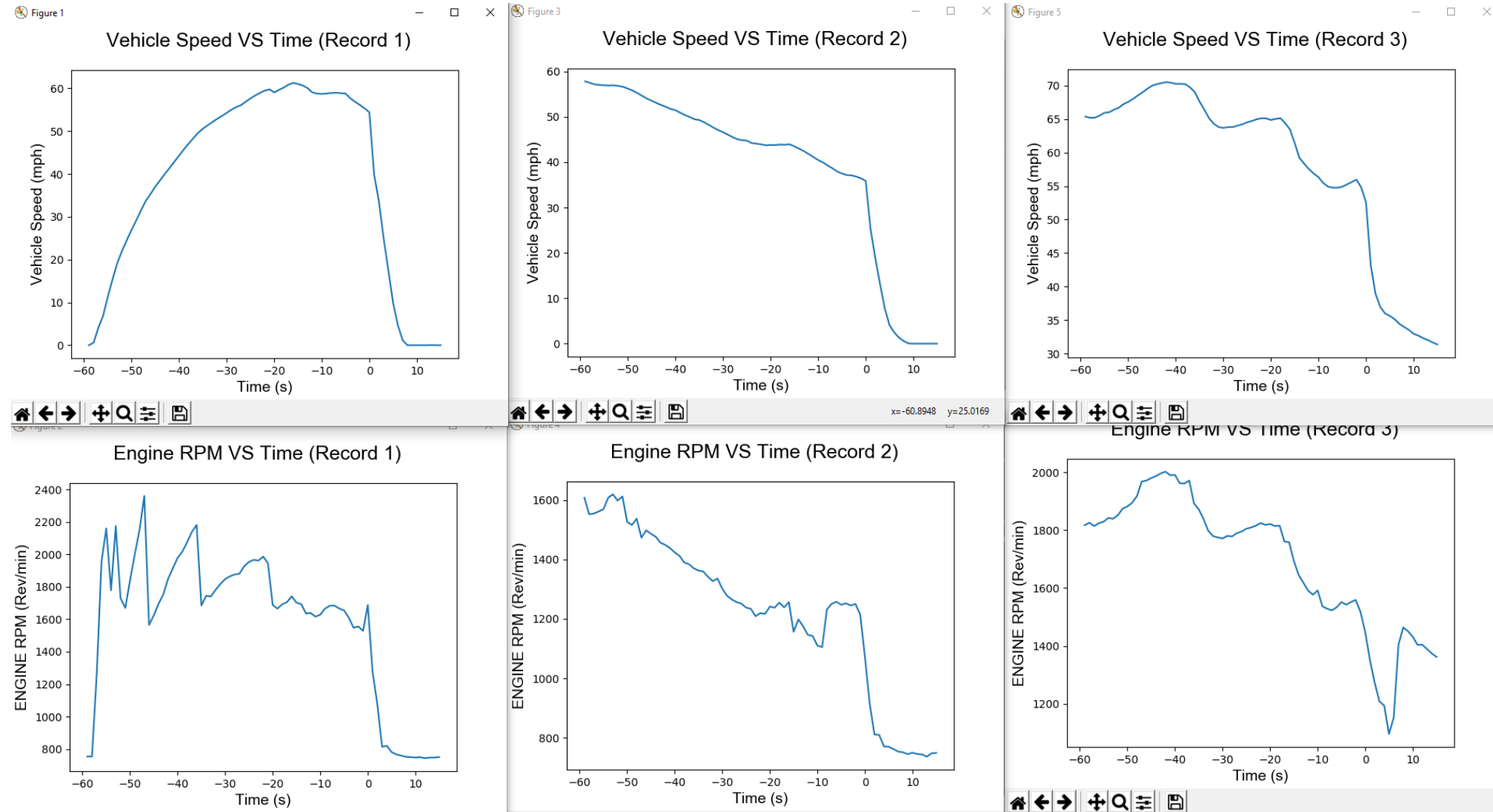
From:
Sent:
To:
Subject:

Duy Van <duyvan1995@gmail.com>
Monday, June 3, 2019 9:21 AM
Daily, Jeremy
Extraction Data from CM2350 S/N 21033060
SN 21033060 SHA 256.txt; red CM2350 6-3-2019.MPC

Received at
9:21

Sent at 9:20

After Data Preservation, Analyze the New Data

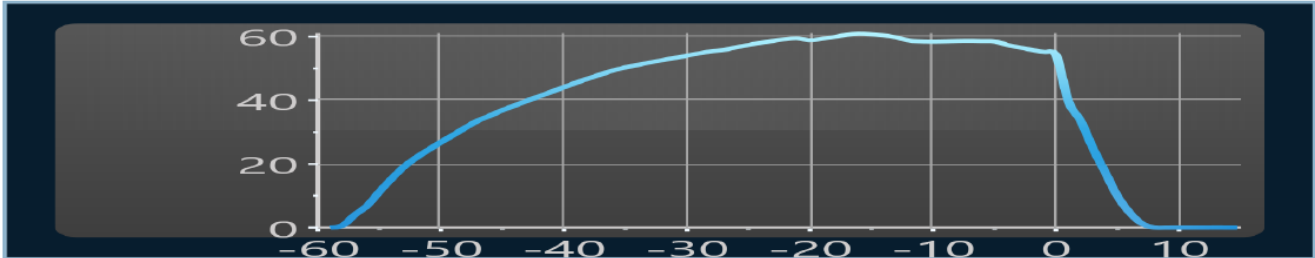


Confirm with PowerSpec

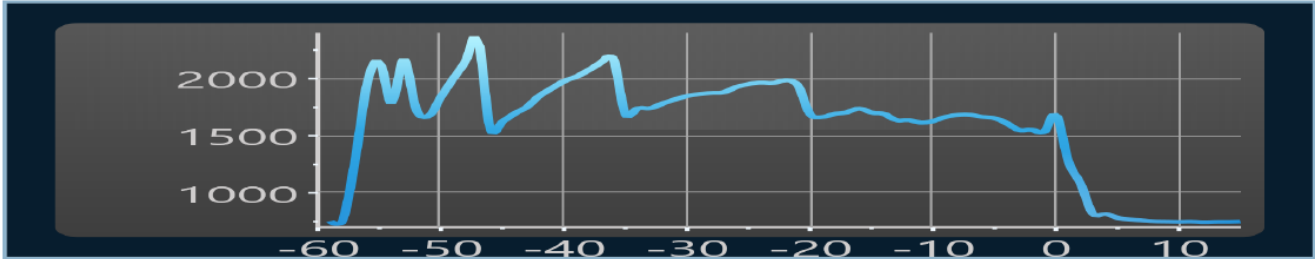
Vehicle Sudden Deceleration Report Record 1

Engine Type	B6.7 2017	Ecm Code	HC80013.14
Engine Serial Number	74109625	Software Phase	22.60.70.3
Unit Number	*****	Extraction Date	06-03-2019 09:46:00
Sudden Decel Threshold Rate:	9.01 mph	ECM Run time	1578:40:56
Occurrence Date: N/A		ECM Run Time at Occurrence: 1287:52:34	
Air Temperature (°F) at Occurrence: 91		Occurrence Distance (mi): 37785.1	

Vehicle Speed



Engine Speed



Percent

Summary and Conclusions

- ECUs may be broken in a crash and not communicate with vehicle networks.
- Board level access provides opportunity to image chips through JTAG programming ports.
- Chip level access reads memory bearing chips directly
- Resulting binary data from Cummins ECUs has Sudden Deceleration Records to decode.
- A man-in-the-middle can help decode the data.
- Data can be manipulated with a hex editor.
- A Secure Hash Algorithm and tight timelines are critical to ensuring forensic verifiability.

Acknowledgments



This material is based upon work supported by the National Science Foundation under Grant No. 1715409. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Autonomous Systems Forensics

Autonomous systems are on the road now

Overview

- What is the ATMA
- Data Overview
- Data Samples
- Key Challenges
- Recommendations
- Summary



Autonomous Truck Mounted Attenuator

https://royaltruckandequipment.com/truck_bodies/autonomous-tma/

https://royaltruckandequipment.com/truck_bodies/autonomous-tma/

The autonomous TMA system can be used in a nearly unlimited variety of applications. Examples include highway maintenance operations including plowing, sweeping, line striping, and water trucks. The ATMA follower system can be configured to follow almost any vehicle as the leader.

In addition to live deployments, many DOTs have worked with universities to conduct live testing and evaluation of the system. These published reports show the potential for the ATMA to bring us closer toward zero deaths.



Tennessee
DOT



North Dakota
DOT



Missouri DOT



Minnesota DOT



Florida DOT



Colorado DOT



Colas U.K. DOT



Caltrans DOT

Leader – Follower System



CDOT Paint Striper as leader



Autonomous Truck Mounted Attenuator as follower

Leader – Follower System



Photo by
John Daily



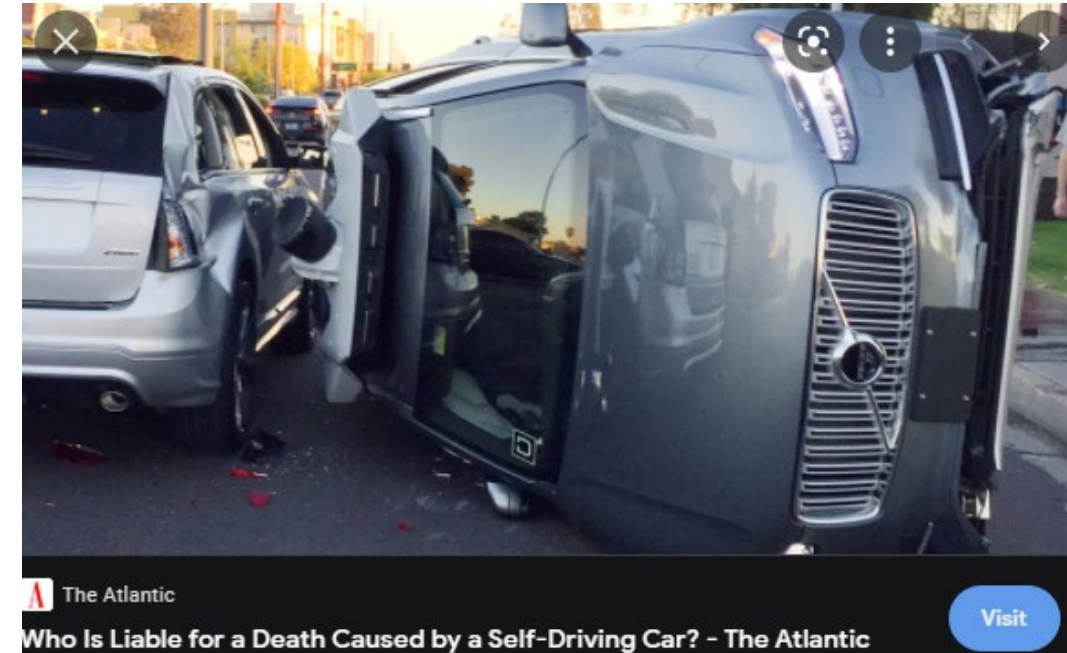
Automated Truck Mounted Attenuator

- Leader sends GPS Based Breadcrumbs
- Follower seeks a following distance along the breadcrumb path

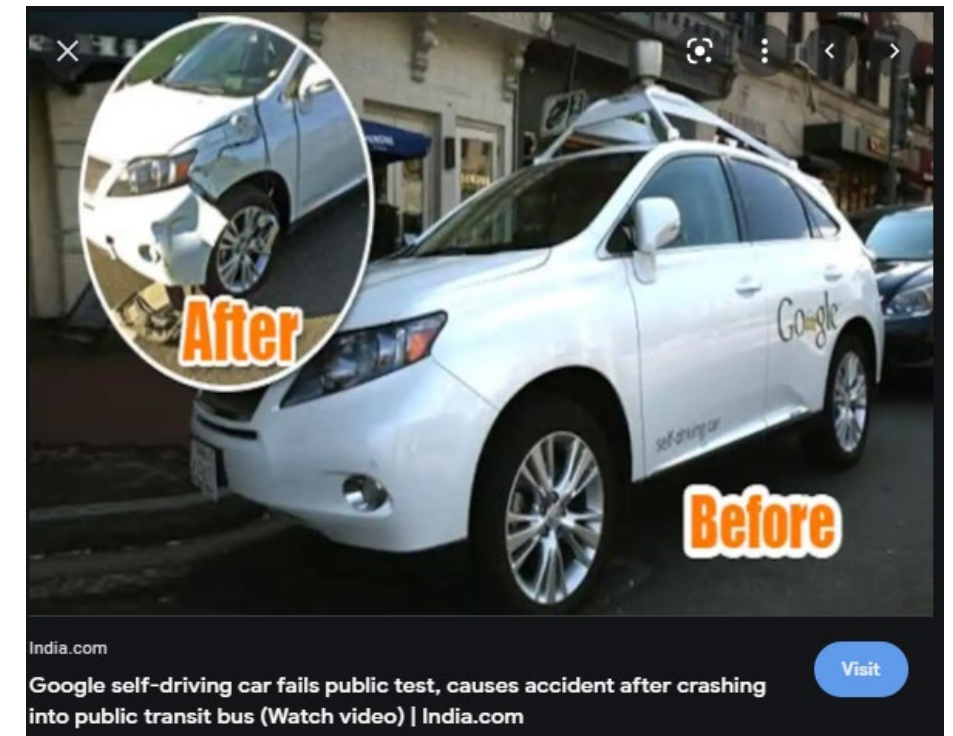
Questions:

- What type of forensic log data exists for these systems?
- Is the data reliable? (Available and accurate)

Motivation



The Atlantic
Who Is Liable for a Death Caused by a Self-Driving Car? - The Atlantic [Visit](#)



India.com
Google self-driving car fails public test, causes accident after crashing into public transit bus (Watch video) | India.com [Visit](#)

ATMA Data Sources

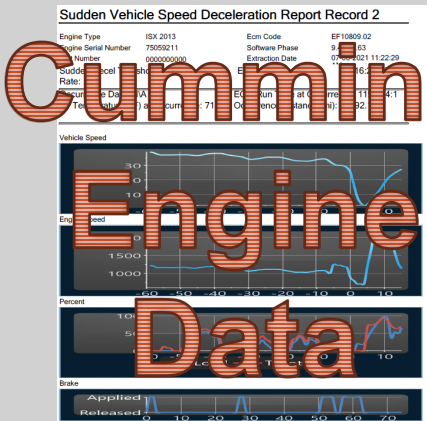
Leader

Follower

Source



Native
Vehicle
J1939

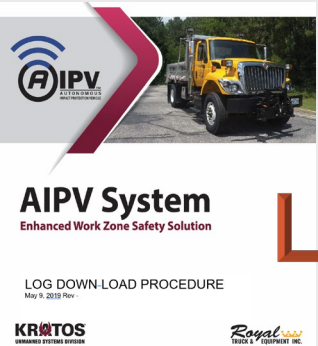


Record 2	Time (Seconds)	Vehicle Speed (mph)	Engine Speed (rpm)	Engine Load (%)	Throttle (%)	Brake Status	Clutch Status	Cruise Status	Lamp Status
-16	33	1030	28.5	35.6	-	-	-	-	-
-15	33	1032	31.4	44.4	-	-	-	-	-
-14	31	1031	38.1	44.4	-	-	-	-	-
-13	31	1031	28.6	44.4	-	-	-	-	-
-12	31	1031	28.6	44.4	-	-	-	-	-
-11	31	1031	28.6	44.4	-	-	-	-	-
-10	31	1031	28.6	44.4	-	-	-	-	-
-9	31	1031	28.6	44.4	-	-	-	-	-
-8	31	1031	28.6	44.4	-	-	-	-	-
-7	31	1031	28.6	44.4	-	-	-	-	-
-6	31	1031	28.6	44.4	-	-	-	-	-
-5	31	1031	28.6	44.4	-	-	-	-	-
-4	31	1031	28.6	44.4	-	-	-	-	-
-3	31	1031	28.6	44.4	-	-	-	-	-
-2	31	1031	28.6	44.4	-	-	-	-	-
-1	31	1031	28.6	44.4	-	-	-	-	-
0	31	1031	28.6	44.4	-	-	-	-	-
1	31	1031	28.6	44.4	-	-	-	-	-
2	31	1031	28.6	44.4	-	-	-	-	-
3	31	1031	28.6	44.4	-	-	-	-	-
4	31	1031	28.6	44.4	-	-	-	-	-
5	31	1031	28.6	44.4	-	-	-	-	-
6	31	1031	28.6	44.4	-	-	-	-	-
7	31	1031	28.6	44.4	-	-	-	-	-
8	31	1031	28.6	44.4	-	-	-	-	-
9	31	1031	28.6	44.4	-	-	-	-	-
10	31	1031	28.6	44.4	-	-	-	-	-
11	31	1031	28.6	44.4	-	-	-	-	-
12	31	1031	28.6	44.4	-	-	-	-	-
13	31	1031	28.6	44.4	-	-	-	-	-
14	31	1031	28.6	44.4	-	-	-	-	-
15	31	1031	28.6	44.4	-	-	-	-	-

Brake
Data
Recorder



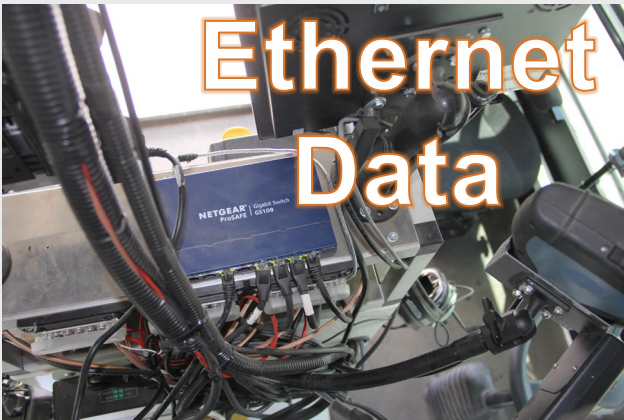
Autonomy
Solution



LOG FILES



Ethernet
Data



ATMA Onboard Data Overview

- Data Sources:
 - Native Vehicle data – Available via J1939 standard interface. Includes log files for engine ECU, transmission, and brake controller
 - ATMA specific log files – Log files generated from ATMA specific commands and navigation information

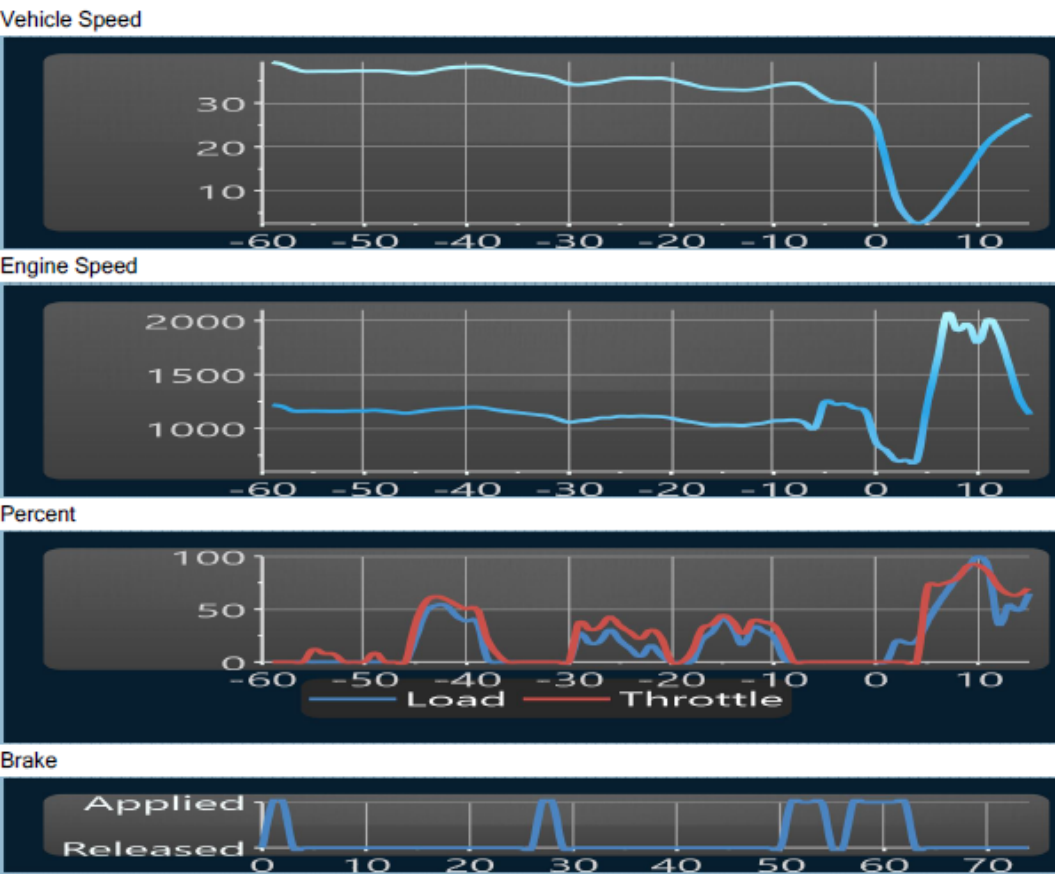


Native vehicle Data Sample:

- Data captured through the leader's diagnostic port using Cummins Powerspec software
- Data collection performed on 6 July 2021
- Shows leader vehicle events
 - Brake
 - Accelerator pedal
 - Vehicle Speed
 - Engine RPM
- Common for incident response

Sudden Vehicle Speed Deceleration Report Record 2

Engine Type	ISX 2013	Ecm Code	EF10809.02
Engine Serial Number	75059211	Software Phase	9.40.17.63
Unit Number	0000000000	Extraction Date	07-06-2021 11:22:29
Sudden Decel Threshold Rate:	7.00 mph/s	ECM Run time	1216:20:12
Occurrence Date: N/A	ECM Run Time at Occurrence: 1190:44:1		
Air Temperature (°F) at Occurrence: 71	Occurrence Distance (mi): 20092.1		



Record 2

Time (Seconds)	Vehicle Speed (mph)	Engine Speed (rpm)	Engine Load (%)	Throttle (%)	Brake Status	Clutch Status	Cruise Status	Lamp Status
-16	33	1030	28.5	35.6	-	-	-	-
-15	33	1032	41.4	44.4	-	-	-	-
-14	33	1031	32.8	38.4	-	-	-	-
-13	33	1026	15.2	26.0	-	-	-	-
-12	33	1039	33.6	39.6	-	-	-	-
-11	33	1049	29.3	37.6	-	-	-	-
-10	34	1069	23.8	34.8	-	-	-	-
-9	34	1072	3.1	19.2	-	-	-	-
-8	34	1078	0.0	0.0	On	-	-	-
-7	34	1054	0.0	0.0	On	-	-	-
-6	33	996	0.0	0.0	On	-	-	-
-5	31	1251	0.0	0.0	On	-	-	-
-4	30	1222	0.0	0.0	-	-	-	-
-3	30	1230	0.0	0.0	-	-	-	-
-2	30	1185	0.0	0.0	On	-	-	-
-1	28	1158	0.0	0.0	On	-	-	-
0	25	872	0.0	0.0	On	-	-	-
1	17	796	0.0	0.0	On	-	-	-
2	8	699	19.9	0.0	On	-	-	-
3	4	710	17.6	0.0	On	-	-	-
4	3	701	19.5	0.0	-	-	-	-
5	3	1215	37.5	69.2	-	-	-	-
6	6	1633	53.9	72.4	-	-	-	-
7	9	2076	67.6	75.2	-	-	-	-
8	11	1898	80.9	79.6	-	-	-	-
9	15	1981	89.5	91.2	-	-	-	-
10	18	1780	100.0	91.6	-	-	-	-
11	21	2023	88.3	84.8	-	-	-	-
12	23	1875	35.2	70.8	-	-	-	-
13	25	1588	54.7	64.0	-	-	-	-
14	26	1286	47.7	63.6	-	-	-	-
15	27	1138	65.2	70.8	-	-	-	-

ATMA Log Data Sample:



AIPV System
Enhanced Work Zone Safety Solution

LOG DOWN-LOAD PROCEDURE
May 9, 2019 Rev -



Data Headers available in the .CSV log files downloaded from the ATMA Limon System in January 2022 testing

Table 1. Data Headers from ATMA CSV Log File

Vehicle	Crumb	Stamp	Lat	Lon	Alt	Heading	Heading (Desired)	Velocity
Velocity (Desired)	Gap	Gap (Desired)	#of Satellites	Valid	CTE	Accel	Steer	State

ATMA Log Data Sample:

wer - CDOT_TEST_DAY3 > CDOT_TEST_DAY3 > ASTOP_9MPH > RUN1 > FOLLOWER

Name

CDOT_ASTOP_9MPH_RUN1_2021-04-08_14-08-36_nav

follower

follower

gps

nav

overhe

timeset

Is this based on GPS or System Clock?

follower - Notepad

File Edit Format View Help
FLW_OFFSETS,0.000,0.000,0.025,2,1.200,0.000
Heading PID:2.200,0.000,0.000, 0.0000, 0.0000, 0.0000
CTE PID:0.000,0.000,0.000, 0.0000, 0.0000, 0.0000
Waiting for leader Go
level=2; description=Adjacent Object Detected; sensor=LIDAR; fram
LDR_OFFSETS,0.000,0.000,0.025,1,1.168,0.000,0.000
LDR, stamp=14085110, dra_time=0.0000, dra_distance=0.0000, lat=37.442
NAV, stamp=14085120, dra_time=0.00, dra_distance=0.00, lat=37.442
FLW_OFFSETS,0.000,0.000,0.025,2,1.200,0.000
Heading PID:2.200,0.000,0.000, 0.0000, 0.0000, 0.0000
CTE PID:0.000,0.000,0.000, 0.0000, 0.0000, 0.0000
Waiting for leader Go
level=2; description=Adjacent Object Detected; sensor=LIDAR; fram
NAV, stamp=14085130, dra_time=0.00, dra_distance=0.00, lat=37.442
Last VCR=14085110;This VCR=14085120;took(ms)=137.23
Checking nav; nav_time=14085120
LDR_OFFSETS,0.000,0.000,0.025,1,1.168,0.000,0.000
LDR, stamp=14085120, dra_time=0.00, dra_distance=0.00, lat=37.4425
NAV, stamp=14085140, dra_time=0.00, dra_distance=0.00, lat=37.44281318, lon=-105.85716268, alt=2281.4
FLW_OFFSETS,0.000,0.000,0.025,2,1.200,0.000
Heading PID:2.200,0.000,0.000, 0.0000, 0.0000, 0.0000
CTE PID:0.000,0.000,0.000, 0.0000, 0.0000, 0.0000

These data raise questions regarding timing, accuracy, and source.

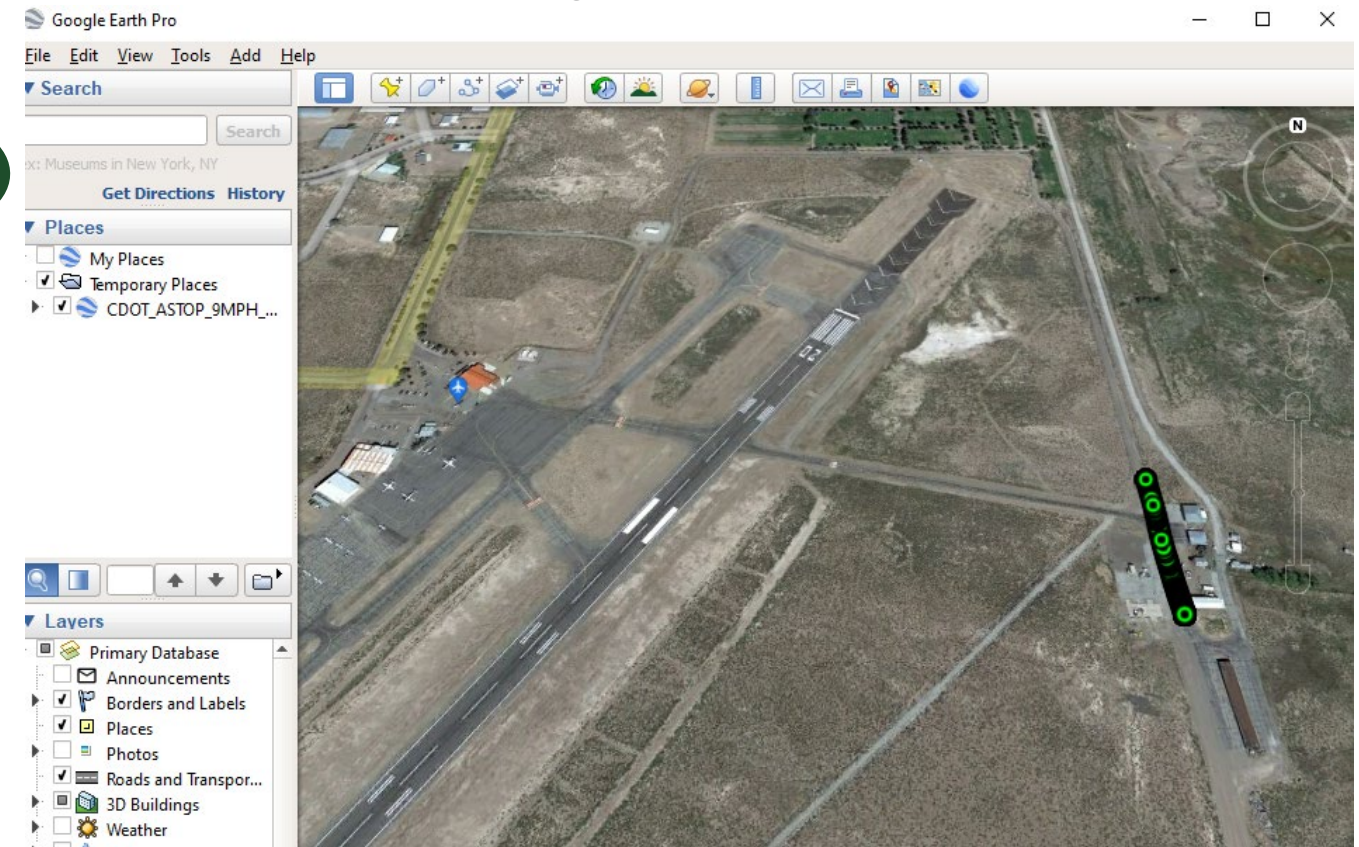
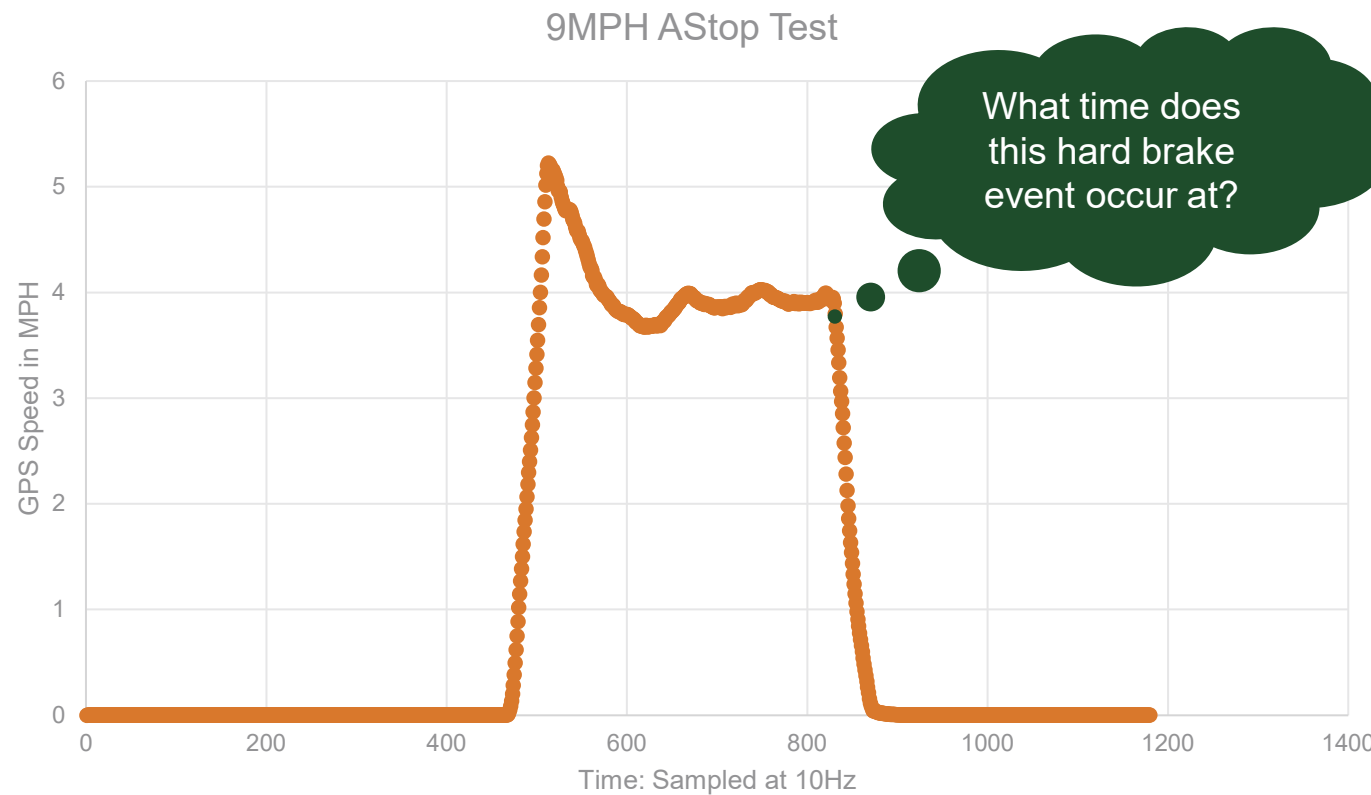
gps - Notepad

File Edit Format View Help
GPS_POS,0.0977, 14070330,0,26, 37.442813117,-105.857150083,2281.765,0,
VCR, 14070330, 3, 3, 14,5.8460,19.8690,24.9240,0.0070,0.0140,0.0140,0
3, 14,5.8440,19.8680,24.9260,0.0070,0.0140,0.0140,0
70340,0,26, 37.442813117,-105.857150083,2281.765,0,
70350,0,26, 37.442813117,-105.857150083,2281.765,0,
3, 14,5.8460,19.8710,24.9220,0.0070,0.0140,0.0140,0
70360,0,26, 37.442813117,-105.857150083,2281.765,0,
3, 14,5.8460,19.8680,24.9250,0.0070,0.0140,0.0150,0
70370,0,26, 37.442813117,-105.857150083,2281.765,0,
3, 14,5.8450,19.8690,24.9250,0.0070,0.0140,0.0150,0
70380,0,26, 37.442813117,-105.857150083,2281.764,0,
3, 14,5.8460,19.8710,24.9220,0.0080,0.0150,0.0160,0
70390,0,26, 37.442813117,-105.857150083,2281.765,0,
3, 14,5.8420,19.8680,24.9290,0.0080,0.0150,0.0160,0
70400,0,26, 37.442813133,-105.857150083,2281.764,0,
VCR, 14070390, 3, 3, 14,5.8460,19.8710,24.9220,0.0080,0.0150,0.0160,0
GPS_POS,0.0791, 14070410,0,26, 37.442813133,-105.857150083,2281.762,0,
VCR, 14070400, 3, 3, 14,5.8470,19.8720,24.9220,0.0080,0.0150,0.0160,0
GPS_POS,0.1041, 14070420,0,26, 37.442813133,-105.857150083,2281.761,0,

TIME	VEH	CRUMB	STAMP	LAT	LON	ALT	HDG	(Desired)	VELOCITY	(Desired)	GAP	(Desired)	#SATS	VALID	CTE	ACCEL	STEER	STATE
38:17.0	FLW	457	20381700	39.27197	-103.7308	1632.171	285.99	286.153	17.69	17.91	48.88	30.5	27	1	0.41	53.59	-3.95	RUN
38:17.1	LDR	476	20381690	39.27213	-103.7315	1630.346	286.4	17.79	286.3	400	77							
38:17.1	FLW	457	20381710	39.27198	-103.7308	1632.173	285.86	286.143	17.67	17.82	48.89	30.5	27	1	0.42	52.99	-4.27	RUN
38:17.2	LDR	477	20381700	39.27213	-103.7315	1630.347	286.41	17.77	286.8	401	77							
38:17.2	FLW	457	20381720	39.27198	-103.7309	1632.18	285.84	286.146	17.85	17.78	48.9	30.5	27	1	0.43	50.74	-4.33	RUN
38:17.2	LDR	478	20381710	39.27213	-103.7315	1630.34	286.39	17.94	285.6	402	77							
38:17.3	FLW	457	20381730	39.27198	-103.7309	1632.175	285.87	286.15	18.08	17.85	48.9	30.5	27	1	0.43	49.3	-4.26	RUN
38:17.3	LDR	479	20381720	39.27214	-103.7315	1630.339	286.33	17.9	286.3	403	77							
38:17.4	FLW	457	20381740	39.27198	-103.7309	1632.184	285.86	286.148	18.16	17.92	48.9	30.5	27	1	0.42	49.25	-4.18	RUN
38:17.5	LDR	480	20381730	39.27214	-103.7316	1630.341	286.31	17.82	287.1	404	77							
38:17.5	FLW	457	20381750	39.27198	-103.7309	1632.189	285.8	286.153	18.19	17.86	48.89	30.5	27	1	0.43	48.29	-4.33	RUN

ATMA Data Analysis (Initial):

- Cursory Analysis of the logs generates the following:
 - Scatter plot analysis of the GPS Speed vs Timestamp in Excel
 - Google Earth can import .csv or .kml file data and plot a breadcrumb trace of Lat vs Long



- NOTE: Kratos has provided a Python script for automating some of this analysis but at this time further investigation and troubleshooting is being performed on its use.
 - Of specific interest is a method to combine leader and follower logs to generate a combined location breadcrumb path trace

Key Challenge: Data Attribution

- Incident Response to a crash for traditional heavy vehicles has well defined procedures
 - Law Enforcement and investigators are familiar with procedures to download vehicle log files via the standard J1939 interfaces
- Procedures for incident response to autonomous heavy vehicles are in their infancy
 - ATMA specific log data download procedures are new and unfamiliar for law enforcement and investigators
 - Area for Improvement 3.2 from the Tabletop: Streamline and provide data download and handling procedures
- **Issue:** Lack of Common Data Fields Between Powertrain Data Logs and ATMA Data Logs
 - Powertrain data does NOT include a Timestamp – uses Engine Hours for time reference
 - Attribution can also be made using odometer readings
 - ATMA specific logs do NOT include any vehicle network data
 - Wheel Speed should correlate to GPS speed
 - At low speeds wheel speed may be more accurate
 - Currently, these signals are not synchronized

Table 1. Data Headers from ATMA CSV Log File

Vehicle	Crumb	Stamp	Lat	Lon	Alt	Heading	Heading (Desired)	Velocity
Velocity (Desired)	Gap	Gap (Desired)	#of Satellites	Valid	CTE	Accel	Steer	State

Powerspec Data Header

Time (Seconds)	Vehicle Speed (mph)	Engine Speed (rpm)	Engine Load (%)	Throttle (%)	Brake Status	Clutch Status	Cruise Status	Lamp Status
-----------------	---------------------	--------------------	-----------------	--------------	--------------	---------------	---------------	-------------

NOTE: This time is counting down to Captured Event, not a GPS Time

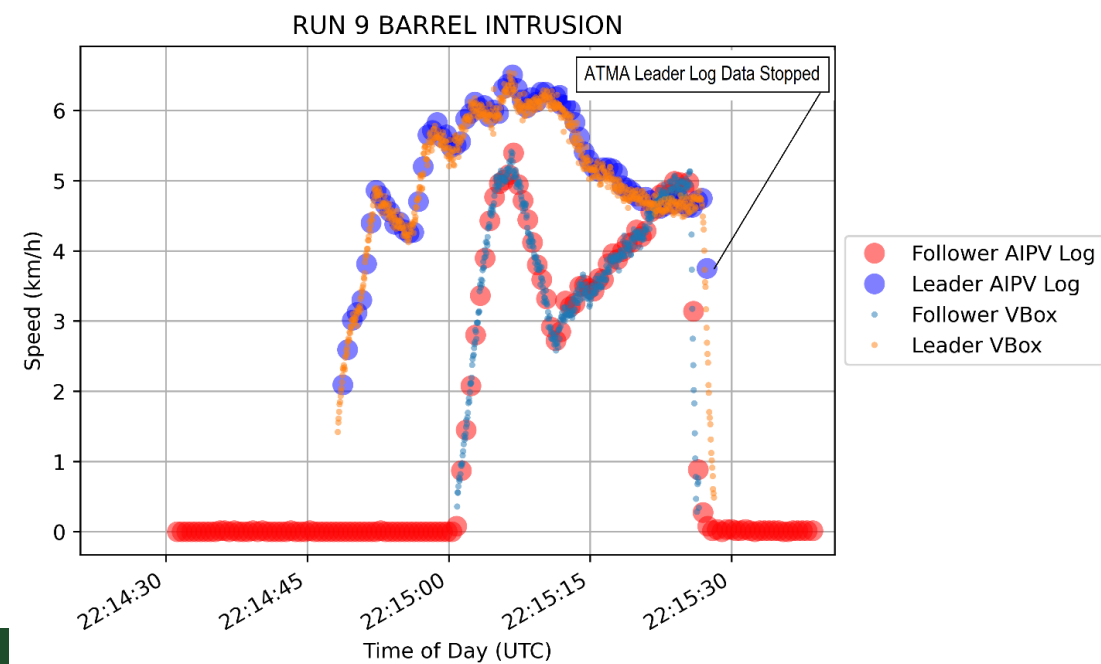
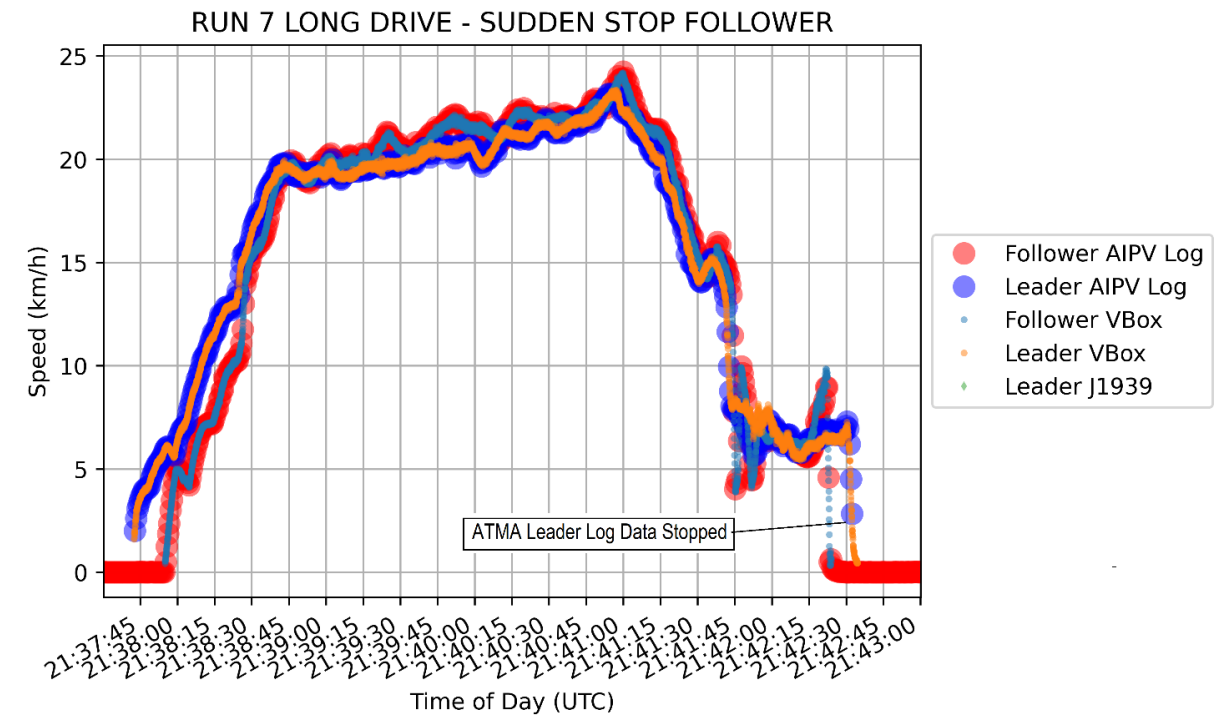
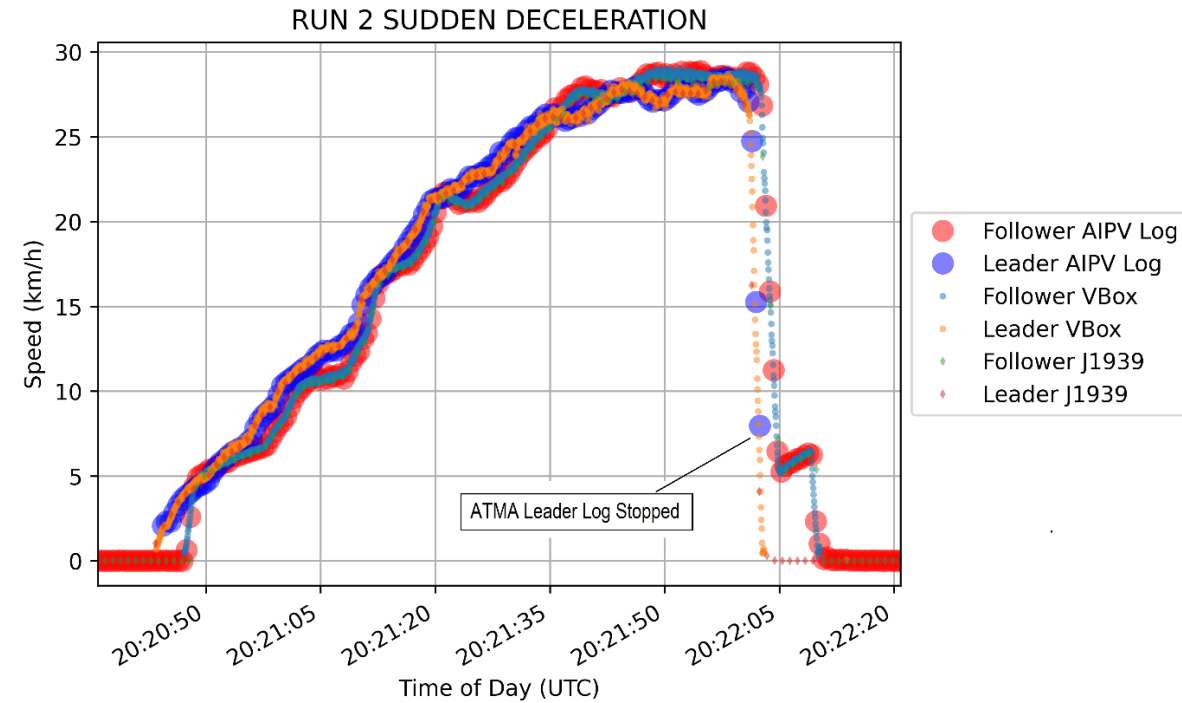
CSU ATMA Data Collection Testing

13 Jan 2022

- **Test 1 – Sudden Deceleration – Leader Initiated Heavy Braking**
- **Test 2 – Sudden Deceleration – ESTOP Leader**
- **Test 3 – Sudden Deceleration – ESTOP Follower**
- **Test 4 – Uncommanded Sudden Stop from Follower**
- **Test 5 – Sudden Deceleration – Barrel Intrusion**



Test Result Data Samples



Data and Security Recommendations:

Recommendation 1: Improve data attribution -- Add vehicle specific data sources to ATMA specific log to facilitate direct comparison to vehicle network data logs.

Recommendation 2: Produce clear and concise ATMA data retrieval procedures – In accordance with the Tabletop After Action Report, Area for Improvement 3.2 highlights the need for clear data download and handling procedures, written for DOT personnel, law enforcement, and other investigators.

Recommendation 3: Deliver a user friendly ATMA log analysis tool – current ATMA log file analysis is cumbersome and does not have a GUI or user-friendly interface to generate plots, charts, and tables of relevant data for incident response.

Recommendation 4: Clarify roles for support to interpret log files – Are there any contractual obligations for ATMA vendor to support the gathering or interpreting log files after an incident?

Recommendation 5: Modify the ATMA logging system to continue to log after an ESTOP– testing showed the ATMA logs terminate upon the loss of ignition power in an ESTOP. The data during the commanded Estop hard braking event is critical information in the case of an accident

Recommendation 1: Improve Data Attribution

- Currently ATMA logs do not include vehicle specific CAN Bus data from J1939.
 - This is challenging for correlating powertrain data to ATMA specific information
- SAE Standard J3197-Automated Driving System Data Logger provides specific recommended minimum data logger data elements for automated driver systems
- Proposed Solution: Add powertrain data to ATMA specific log
 - Can be accomplished via a Data Diode from the J1939 CAN Network to broadcast UDP packets. A data diode would preserve security through physical restriction of a one- way data flow

Sudden Vehicle Speed Deceleration Report Record 1

Engine Type	ISX 2013	Ecm Code	EF10809.02
Engine Serial Number	75059211	Software Phase	9.40.17.63
Unit Number	0000000000	Extraction Date	01-13-2022 01:07:10
Sudden Decel Threshold	7.00 mph/s	ECM Run time	1363:46:32
Rate:		ECM Run Time at Occurrence:	1295:32:7
Occurrence Date: N/A		Occurrence Distance (mi):	22176.7
Air Temperature (°F) at Occurrence:	78		



	VEH	CRUMB	STAMP	LAT	LON	ALT	HDG	HDG (Desired)	VELOCITY (Desired)	GAP	GAP (Desired)	#SATS	VALID	CTE	ACCEL	STEER	STATE
17.0 FLW	457	20381700	39.27197	-103.7308	1632.171	285.99	286.153	17.69	17.91	48.88	30.5	27	1	0.41	53.59	-3.95	RUN
17.1 LDR	476	20381690	39.27213	-103.7315	1630.346	286.4	286.3	17.79	17.91	48.88	30.5	27	1	0.41	53.59	-3.95	RUN
17.1 FLW	457	20381710	39.27198	-103.7308	1632.173	285.99	286.143	17.67	17.82	48.89	30.5	27	1	0.42	52.99	-4.27	RUN
17.2 LDR	477	20381700	39.27213	-103.7315	1630.347	286.41	286.8	17.77	17.91	48.88	30.5	27	1	0.41	53.59	-3.95	RUN
17.2 FLW	457	20381720	39.27198	-103.7309	1632.18	285.84	286.146	17.85	17.78	48.9	30.5	27	1	0.43	50.74	-4.33	RUN
17.2 LDR	478	20381710	39.27213	-103.7315	1630.34	286.39	286.6	17.94	17.82	48.89	30.5	27	1	0.42	52.99	-4.27	RUN
17.3 FLW	457	20381730	39.27198	-103.7309	1632.175	285.87	286.15	18.08	17.85	48.9	30.5	27	1	0.43	49.3	-4.26	RUN
17.3 LDR	479	20381720	39.27214	-103.7315	1630.339	286.33	286.3	17.9	17.82	48.89	30.5	27	1	0.43	49.3	-4.26	RUN
17.4 FLW	457	20381740	39.27198	-103.7309	1632.184	285.86	286.148	18.16	17.92	48.9	30.5	27	1	0.42	49.25	-4.18	RUN
17.5 LDR	480	20381730	39.27214	-103.7316	1630.341	286.31	287.1	18.04	17.88	48.89	30.5	27	1	0.43	48.29	-4.33	RUN
17.5 FLW	457	20381750	39.27198	-103.7309	1632.189	285.8	286.153	18.19	17.86	48.89	30.5	27	1	0.43	48.29	-4.33	RUN
17.5 LDR	481	20381740	39.27214	-103.7316	1630.342	286.31	286.5	18.06	17.85	48.86	30.5	27	1	0.44	48.68	-4.39	RUN
17.6 FLW	457	20381760	39.27199	-103.7309	1632.191	285.84	286.154	18.07	17.84	48.82	30.5	27	1	0.43	49.35	-4.33	RUN
17.7 LDR	482	20381750	39.27214	-103.7316	1630.344	286.31	286.6	18.06	17.85	48.86	30.5	27	1	0.44	48.68	-4.39	RUN
17.7 FLW	457	20381770	39.27199	-103.7309	1632.194	285.85	286.156	18.15	17.85	48.86	30.5	27	1	0.44	48.68	-4.39	RUN
17.7 LDR	483	20381760	39.27214	-103.7316	1630.344	286.34	286.2	18.06	17.85	48.86	30.5	27	1	0.44	48.68	-4.39	RUN
17.8 FLW	457	20381780	39.27199	-103.7309	1632.202	285.88	286.155	18.22	17.83	48.85	30.5	27	1	0.45	47.77	-4.35	RUN
17.8 LDR	484	20381770	39.27215	-103.7316	1630.341	286.34	286.6	18.06	17.85	48.86	30.5	27	1	0.44	48.68	-4.39	RUN
17.9 FLW	457	20381790	39.27199	-103.7309	1632.206	285.84	286.154	18.21	17.88	48.83	30.5	27	1	0.44	48.43	-4.41	RUN
17.9 LDR	485	20381780	39.27215	-103.7316	1630.343	286.35	286.7	18.02	17.85	48.86	30.5	27	1	0.44	48.81	-4.33	RUN
18.0 FLW	457	20381800	39.27199	-103.7309	1632.204	285.85	286.155	18.27	17.98	48.82	30.5	27	1	0.44	48.81	-4.33	RUN
18.1 LDR	486	20381790	39.27215	-103.7316	1630.343	286.4	286.6	18.01	18.01	48.81	30.5	26	1	0.44	51.33	-4.14	RUN
18.1 FLW	457	20381810	39.272	-103.7309	1632.205	285.97	286.149	18.05	18.01	48.81	30.5	26	1	0.44	51.33	-4.14	RUN
18.2 LDR	487	20381800	39.27215	-103.7316	1630.342	286.39	286.6	18.06	18.01	48.81	30.5	26	1	0.44	51.11	-4.22	RUN
18.2 FLW	457	20381820	39.272	-103.7309	1632.219	285.94	286.162	18.09	18.03	48.81	30.5	26	1	0.44	51.11	-4.22	RUN
18.3 LDR	488	20381810	39.27215	-103.7316	1630.339	286.4	286.6	18.09	18.03	48.81	30.5	26	1	0.44	51.11	-4.22	RUN
18.3 FLW	457	20381830	39.272	-103.731	1632.225	285.95	286.155	18.02	18.07	48.81	30.5	27	1	0.43	52.26	-4.11	RUN
18.4 LDR	489	20381820	39.27216	-103.7316	1630.34	286.43	286.2	18.18	18.13	48.81	30.5	27	1	0.43	50.47	-3.94	RUN
18.4 FLW	457	20381840	39.272	-103.731	1632.223	285.99	286.146	18.26	18.13	48.81	30.5	27	1	0.43	50.47	-3.94	RUN
18.5 LDR	490	20381830	39.27216	-103.7316	1630.34	286.42	286.3	18.24	18.25	48.79	30.5	27	1	0.44	51.69	-4.13	RUN
18.5 FLW	457	20381850	39.272	-103.731	1632.216	285.97	286.149	18.21	18.21	48.79	30.5	27	1	0.44	51.69	-4.13	RUN
18.6 LDR	491	20381840	39.27216	-103.7316	1630.337	286.42	286.2	18.26	18.25	48.75	30.5	27	1	0.44	53.35	-4.18	RUN
18.6 FLW	457	20381860	39.27201	-103.731	1632.223	285.94	286.15	18.09	18.25	48.75	30.5	27	1	0.44	53.35	-4.18	RUN
18.6 LDR	492	20381850	39.27216	-103.7317	1630.338	286.45	286.3	18.24	18.25	48.8	30.5	27	1	0.43	53.38	-4.04	RUN
18.7 FLW	457	20381870	39.27201	-103.731	1632.23	285.99	286.146	18.09	18.25	48.8	30.5	27	1	0.43	53.38	-4.04	RUN



SURFACE VEHICLE RECOMMENDED PRACTICE	J3197™	J
	Issued	2020-04
	Revised	2021-07
Superseding J3197 APR202		
Automated Driving System Data Logger		

Recommendation 2: Produce Clear and Concise ATMA Data Retrieval Procedures

- Current ATMA log file download procedures are complex and not readily available in the vehicles.
 - Procedure is written for engineers with familiarity in Linux systems
 - Few users are trained on how to accomplish ATMA log file download
 - Current download process uses “root” permission which is a known security vulnerability (See [Security Engineering](#) by Ross Anderson).
 - From the Tabletop AAR Area for Improvement 3.2

“Participating agencies acknowledged the lack of protocols stating what to do with the data that is extracted from the vehicle and how to manage it for further investigation or storage.”
- Procedures should be explicit and clear for download and handling of the data to ensure the integrity of the data if an incident occurs
 - This process will likely mimic existing vehicle data downloads but needs to be explicitly defined for ATMA



AIPV System
Enhanced Work Zone Safety Solution

LOG DOWN-LOAD PROCEDURE
May 9, 2019 Rev -

KRATOS
UNMANNED SYSTEMS DIVISION

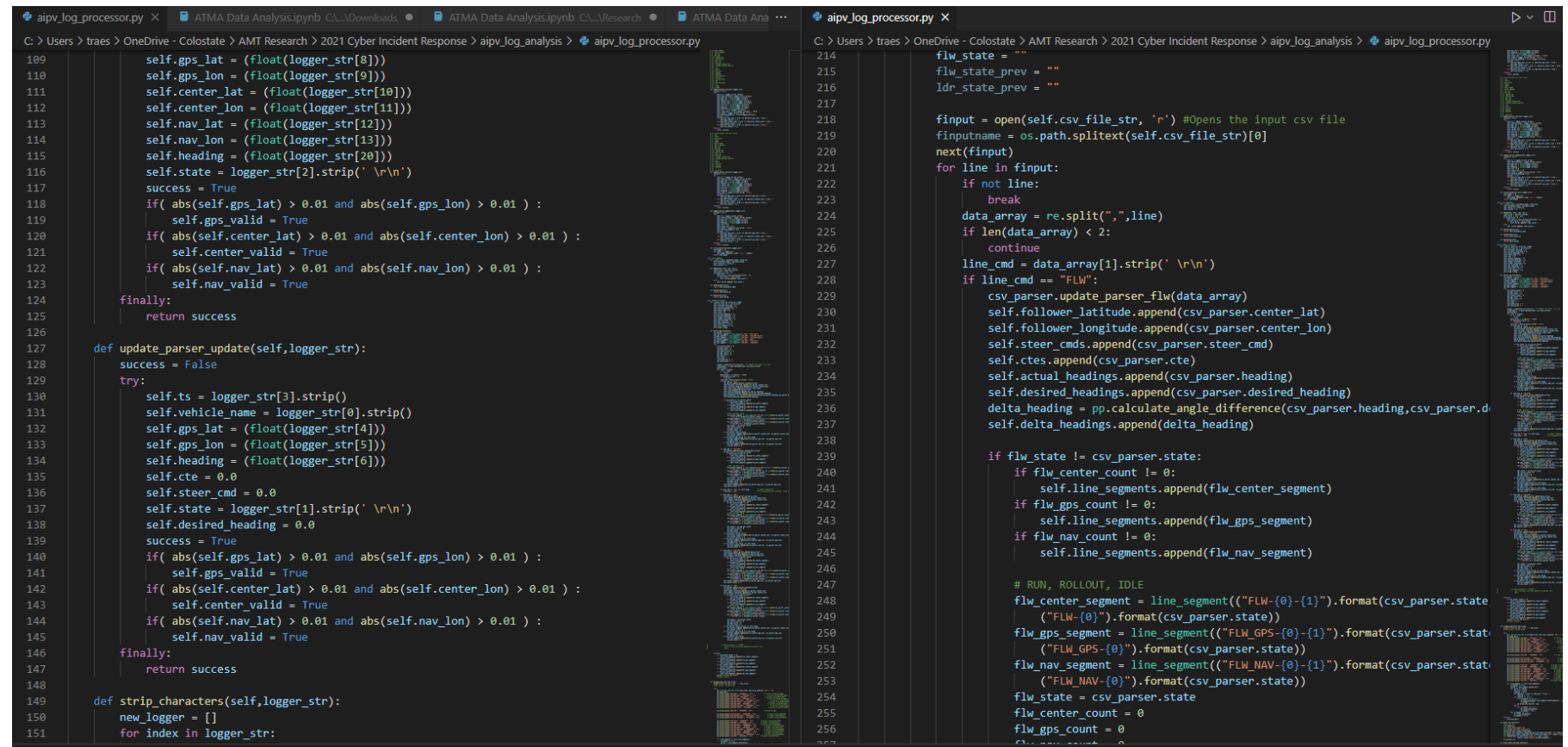
Royal
TRUCK & EQUIPMENT INC.

The screenshot shows the 'Site Manager' application window. On the left, under 'Select Entry:', there is a tree view with 'My Sites' and a sub-entry 'follower_scu'. Below this are buttons for 'New Site', 'New Folder', 'New Bookmark', 'Rename', 'Delete', and 'Duplicate'. On the right, there are tabs for 'General', 'Advanced', 'Transfer Settings', and 'Charset'. The 'General' tab is active, showing fields for 'Host' (192.168.8.1), 'Port' (empty), 'Protocol' (SFTP - SSH File Transfer Protocol), 'Logon Type' (Normal), 'User' (root), and 'Password' (masked with dots). A red circle highlights the 'Logon Type', 'User', and 'Password' fields. Below these are 'Background color' (None) and 'Comments' (empty text area). At the bottom right are 'Connect', 'OK', and 'Cancel' buttons.

Recommendation 3: Deliver a user friendly ATMA log analysis tool

- Current ATMA log analysis is either done with inefficient Excel analysis or a Python script.
 - Many users may not be familiar with python
 - The current Python script requires download of multiple Python add in packages and does not use a GUI

- A GUI based tool could be developed that would create a user-friendly interface to a script to ingest the data logs and produce tables and graphics of interest for an incident
- Log files should be digitally signed to prevent undetected manipulation



The image shows a screenshot of a Python script editor with two files open: `aipv_log_processor.py` and `ATMA Data Analysis.ipynb`. The `aipv_log_processor.py` file contains the following code:

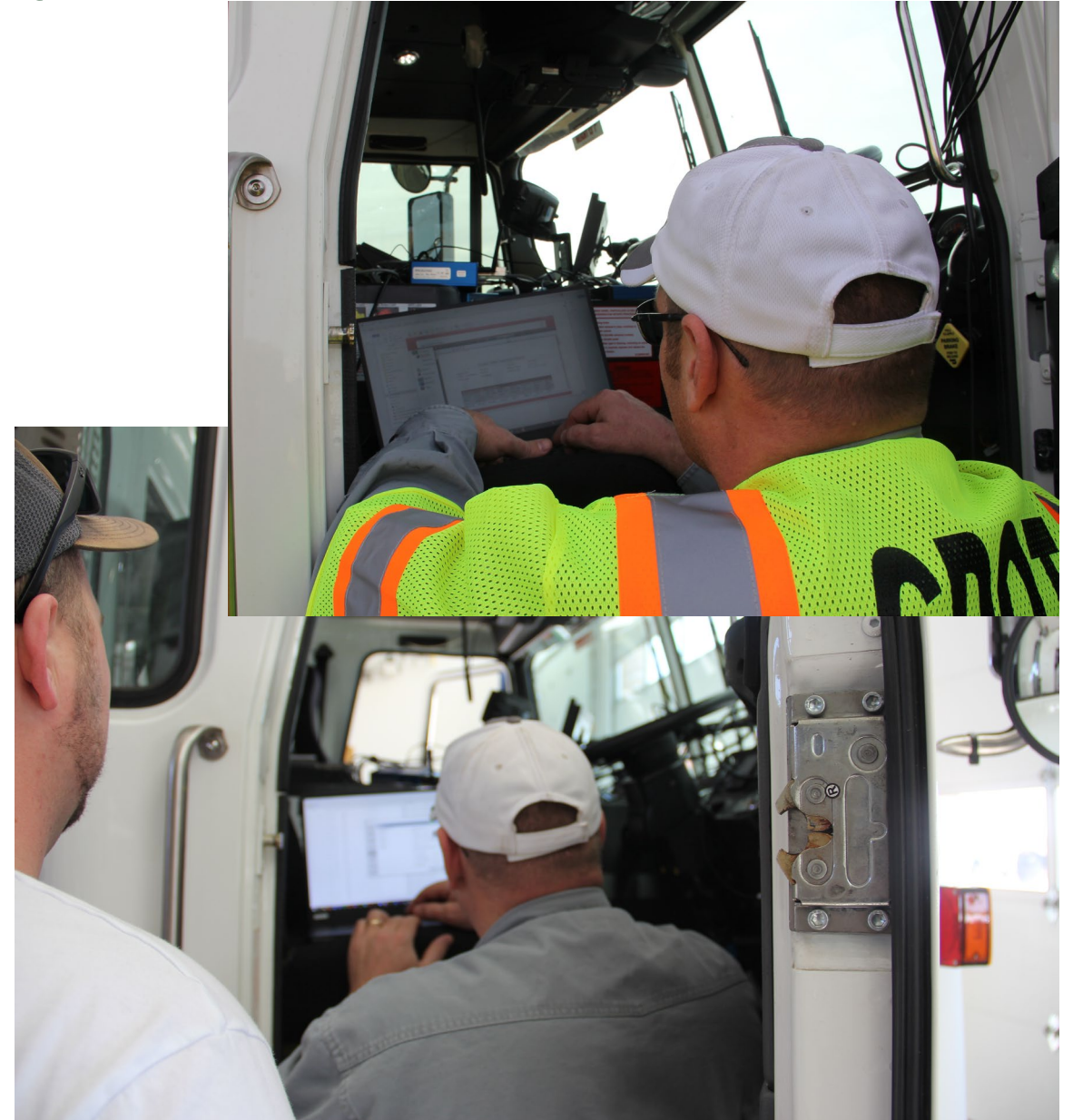
```
109 self.gps_lat = (float(logger_str[8]))
110 self.gps_lon = (float(logger_str[9]))
111 self.center_lat = (float(logger_str[10]))
112 self.center_lon = (float(logger_str[11]))
113 self.nav_lat = (float(logger_str[12]))
114 self.nav_lon = (float(logger_str[13]))
115 self.heading = (float(logger_str[20]))
116 self.state = logger_str[2].strip(' \r\n')
117 success = True
118 if( abs(self.gps_lat) > 0.01 and abs(self.gps_lon) > 0.01 ) :
119     self.gps_valid = True
120 if( abs(self.center_lat) > 0.01 and abs(self.center_lon) > 0.01 ) :
121     self.center_valid = True
122 if( abs(self.nav_lat) > 0.01 and abs(self.nav_lon) > 0.01 ) :
123     self.nav_valid = True
124 finally:
125     return success
126
127 def update_parser_update(self,logger_str):
128     success = False
129     try:
130         self.ts = logger_str[3].strip()
131         self.vehicle_name = logger_str[0].strip()
132         self.gps_lat = (float(logger_str[4]))
133         self.gps_lon = (float(logger_str[5]))
134         self.heading = (float(logger_str[6]))
135         self.cte = 0.0
136         self.steer_cmd = 0.0
137         self.state = logger_str[1].strip(' \r\n')
138         self.desired_heading = 0.0
139         success = True
140         if( abs(self.gps_lat) > 0.01 and abs(self.gps_lon) > 0.01 ) :
141             self.gps_valid = True
142         if( abs(self.center_lat) > 0.01 and abs(self.center_lon) > 0.01 ) :
143             self.center_valid = True
144         if( abs(self.nav_lat) > 0.01 and abs(self.nav_lon) > 0.01 ) :
145             self.nav_valid = True
146     finally:
147         return success
148
149 def strip_characters(self,logger_str):
150     new_logger = []
151     for index in logger_str:
```

The `ATMA Data Analysis.ipynb` file contains the following code:

```
214 flw_state = ""
215 flw_state_prev = ""
216 ldr_state_prev = ""
217
218 finput = open(self.csv_file_str, 'r') #Opens the input csv file
219 finputname = os.path.splitext(self.csv_file_str)[0]
220 next(finput)
221 for line in finput:
222     if not line:
223         break
224     data_array = re.split(",",line)
225     if len(data_array) < 2:
226         continue
227     line_cmd = data_array[1].strip(' \r\n')
228     if line_cmd == "FLW":
229         csv_parser.update_parser_flw(data_array)
230         self.follower_latitude.append(csv_parser.center_lat)
231         self.follower_longitude.append(csv_parser.center_lon)
232         self.steer_cmds.append(csv_parser.steer_cmd)
233         self.ctes.append(csv_parser.cte)
234         self.actual_headings.append(csv_parser.heading)
235         self.desired_headings.append(csv_parser.desired_heading)
236         delta_heading = pp.calculate_angle_difference(csv_parser.heading,csv_parser.d
237         self.delta_headings.append(delta_heading)
238
239     if flw_state != csv_parser.state:
240         if flw_center_count != 0:
241             self.line_segments.append(flw_center_segment)
242         if flw_gps_count != 0:
243             self.line_segments.append(flw_gps_segment)
244         if flw_nav_count != 0:
245             self.line_segments.append(flw_nav_segment)
246
247     # RUN, ROLLOUT, IDLE
248     flw_center_segment = line_segment(("FLW-{0}-{1}").format(csv_parser.state
249     ("FLW-{0}").format(csv_parser.state))
250     flw_gps_segment = line_segment(("FLW_GPS-{0}-{1}").format(csv_parser.stat
251     ("FLW_GPS-{0}").format(csv_parser.state))
252     flw_nav_segment = line_segment(("FLW_NAV-{0}-{1}").format(csv_parser.stat
253     ("FLW_NAV-{0}").format(csv_parser.state))
254     flw_state = csv_parser.state
255     flw_center_count = 0
256     flw_gps_count = 0
257     flw_nav_count = 0
```

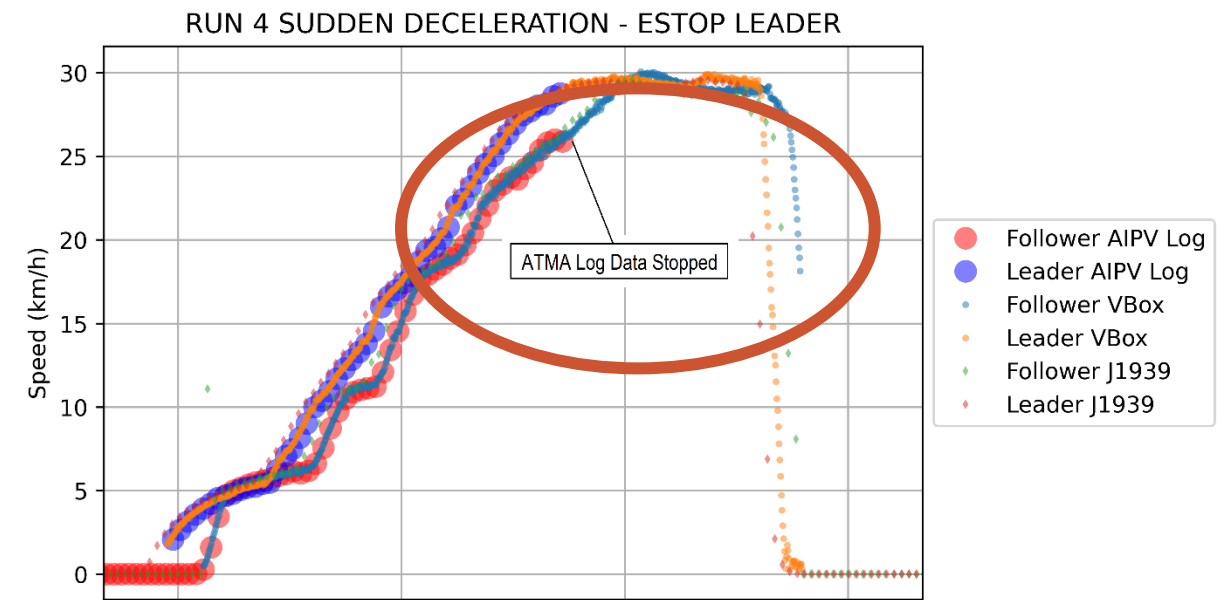
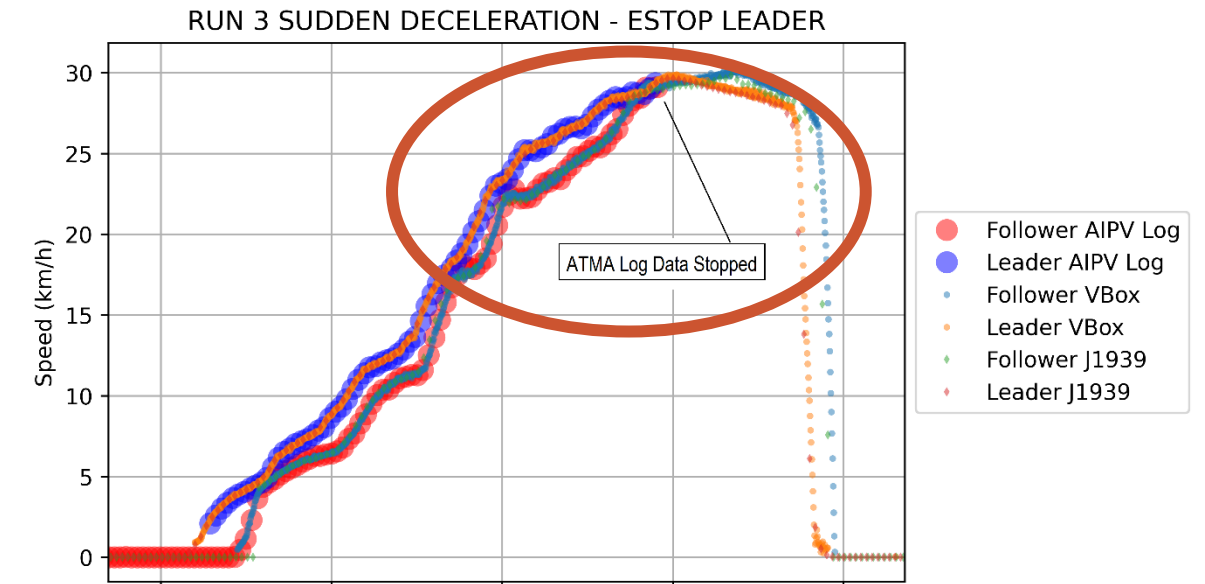
Recommendation 4: Clarify roles for support to interpret log files

- DOT acquisition documents should have specific requirements language of roles and responsibilities for
 - Log data collection
 - Secure log data storage
 - File download procedures
 - Data interpretation and analysis
 - Training for incident response activities
- Understand how to perform these incident response functions without the ATMA vendor (i.e. practice)



Recommendation 5: Modify the ATMA logging system to continue to log after an ESTOP

- CSU tests Executed multipled ESTOP events- during each one the Kratos recording system abruptly terminated after the ESTOP was commanded
 - ESTOP cuts ignition power to the follower vehicle
 - Kratos designed logger to require ignition power to record data
- Data between the commanded ESTOP and the vehicle actually coming to a stop is critical data in the event of an accident



Questions?



Colorado State University