EXTRACTING EVENT DATA FROM MEMORY CHIPS WITHIN A DETROIT DIESEL DDEC V

Jeremy Daily, Andrew Kongs, James Johnson, Jose Corcega

The University of Tulsa

SAE INTERNATIONAL

THE UNIVERSITY of TULSA

Department of Mechanical Engineering

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

Problem Statement

We want to connect to a truck…

…and get data.

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

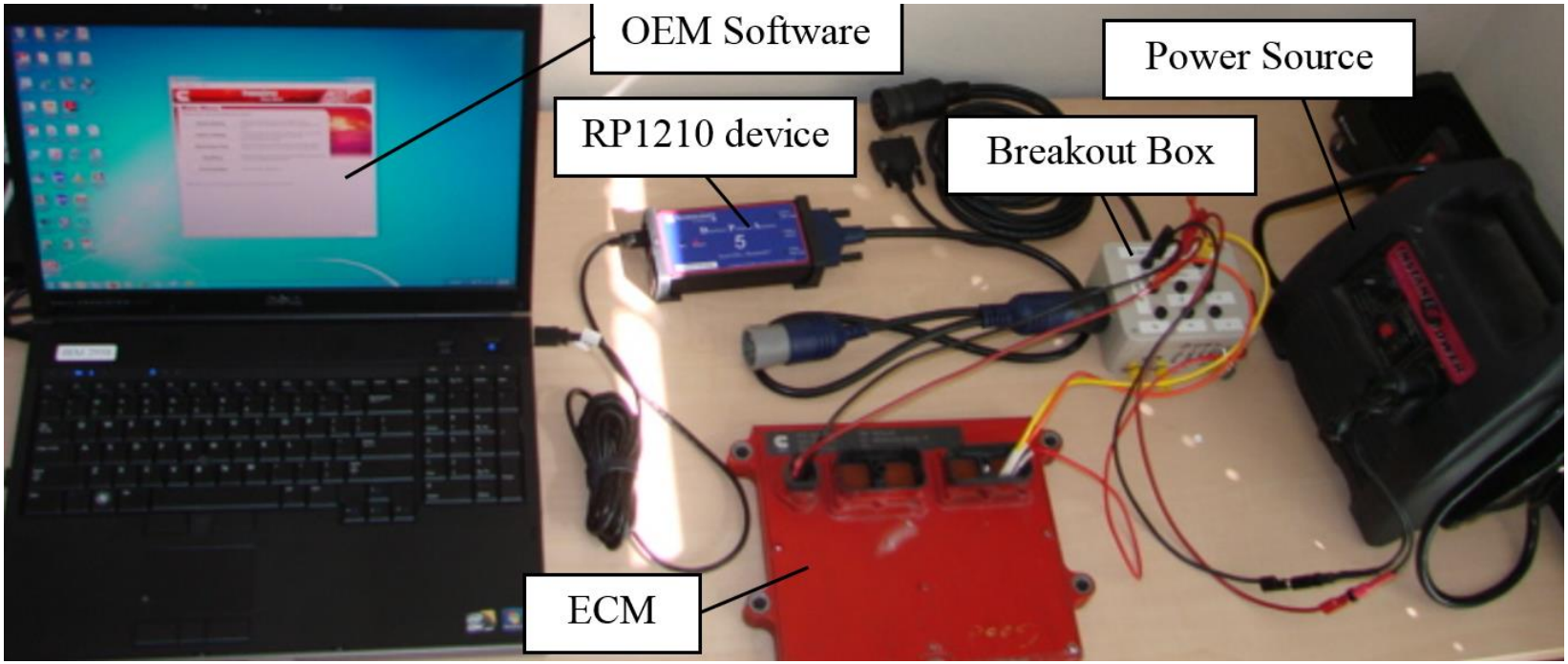
Time	Vehicle Speed (mph)	Engine Speed (rpm)	Brake	Clutch	Engine Load (%)	Throttle (%)	Cruise	Diag. Code
-0:59	23.5	0	No	No	0.00	0.00	No	Yes
-0:58	22.0	0	No	No	0.00	0.00	No	Yes
-0:57	20.0	0	No	No	0.00	0.00	No	Yes
-0:56	18.0	0	No	No	0.00	0.00	No	Yes
-0:55	16.0	0	No	No	0.00	0.00	No	Yes
-0:54	14.0	0	No	No	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.

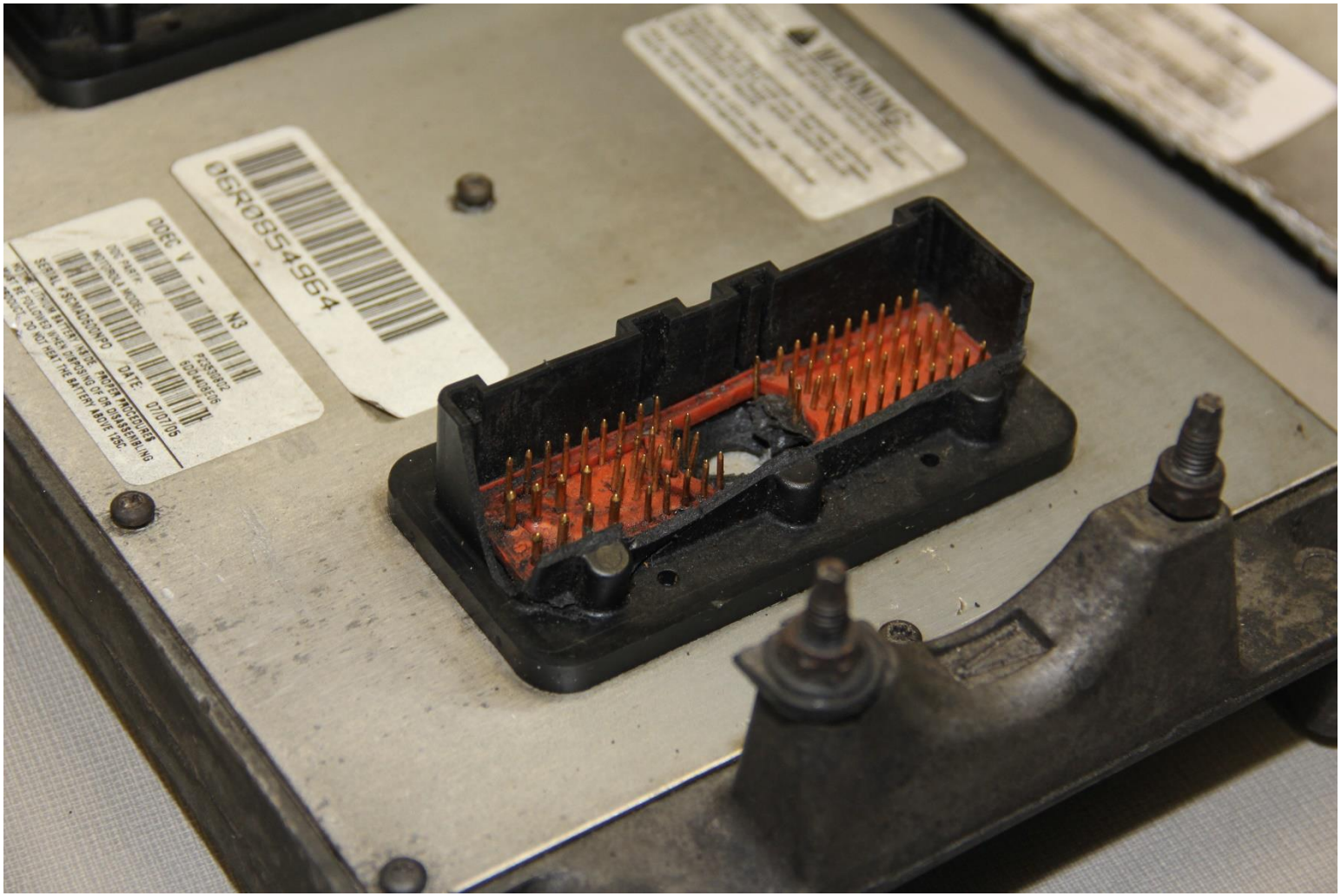


Bench Top Download (Fault Free)

But, sometimes it's not that easy.

The electrical system is compromised.

Recovered Modules



Attempted Download

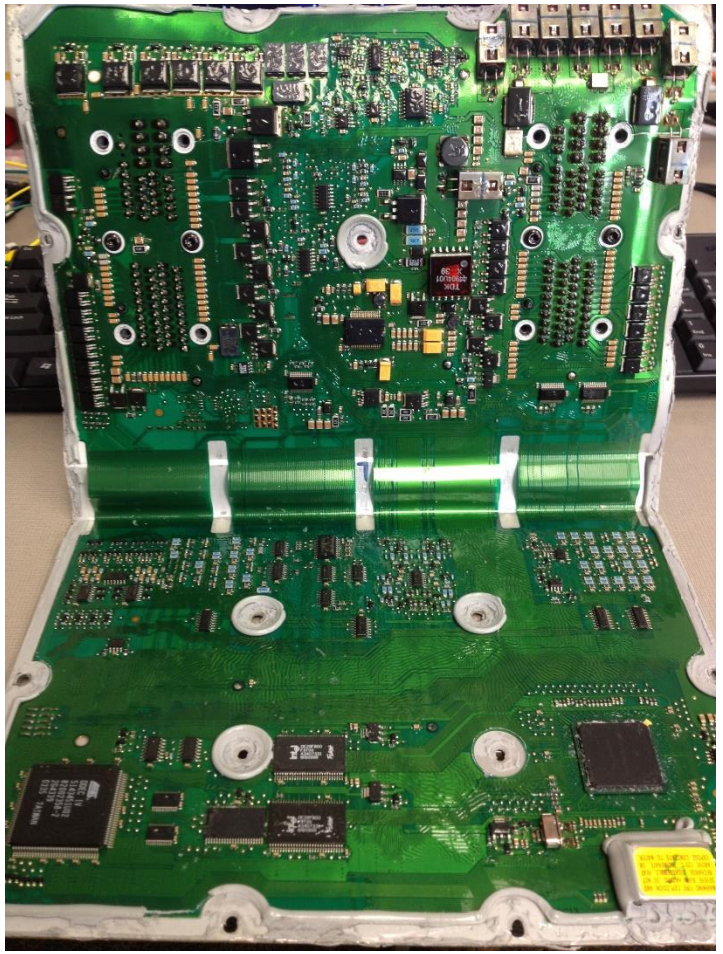
Able to connect, but throws a J1708 Network Error??

This isn't covered in the manual…

Let's take a peek inside the module.

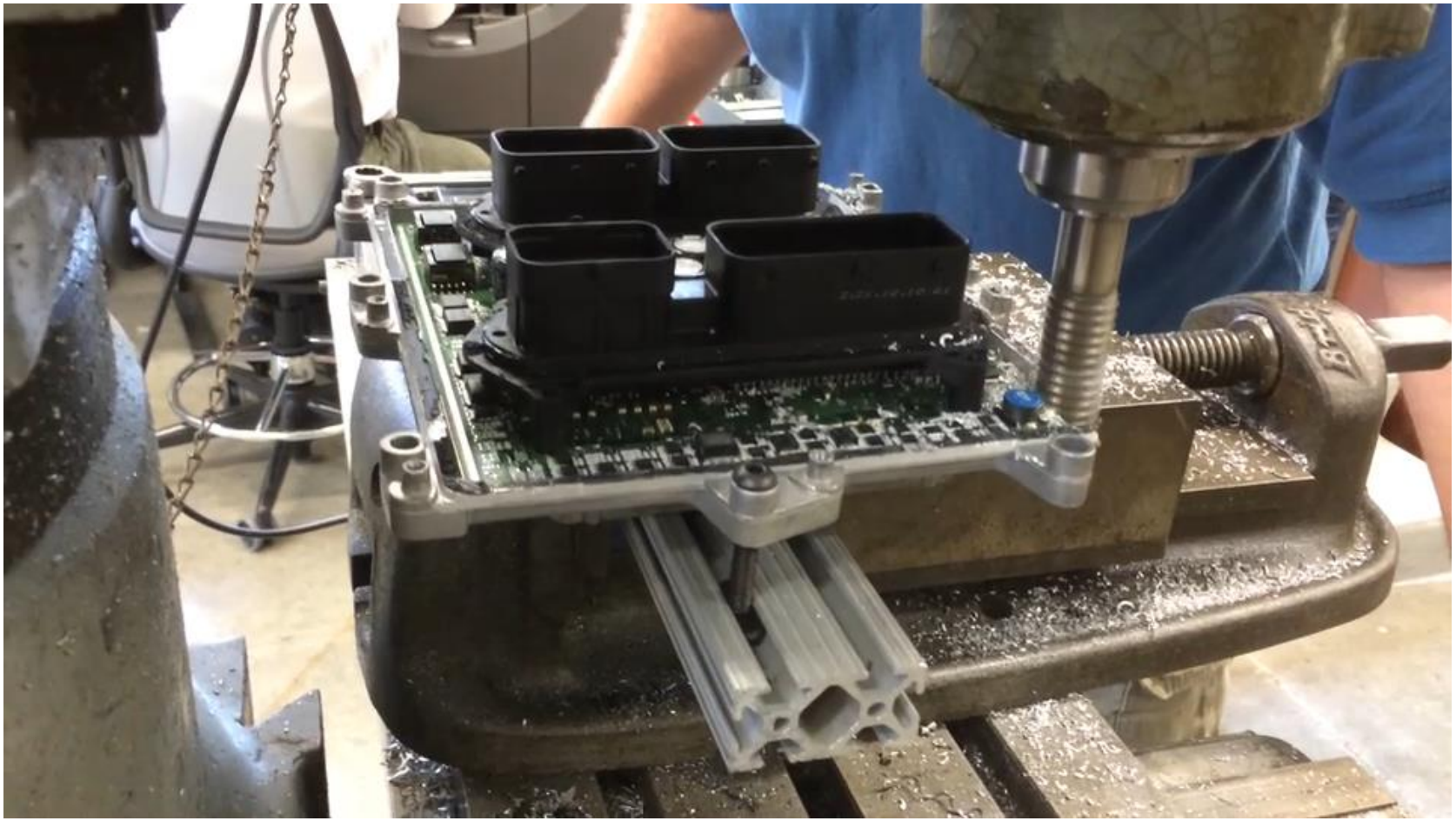
Chip Access

Accessing the chips the mechanical engineering way…



Chip Access

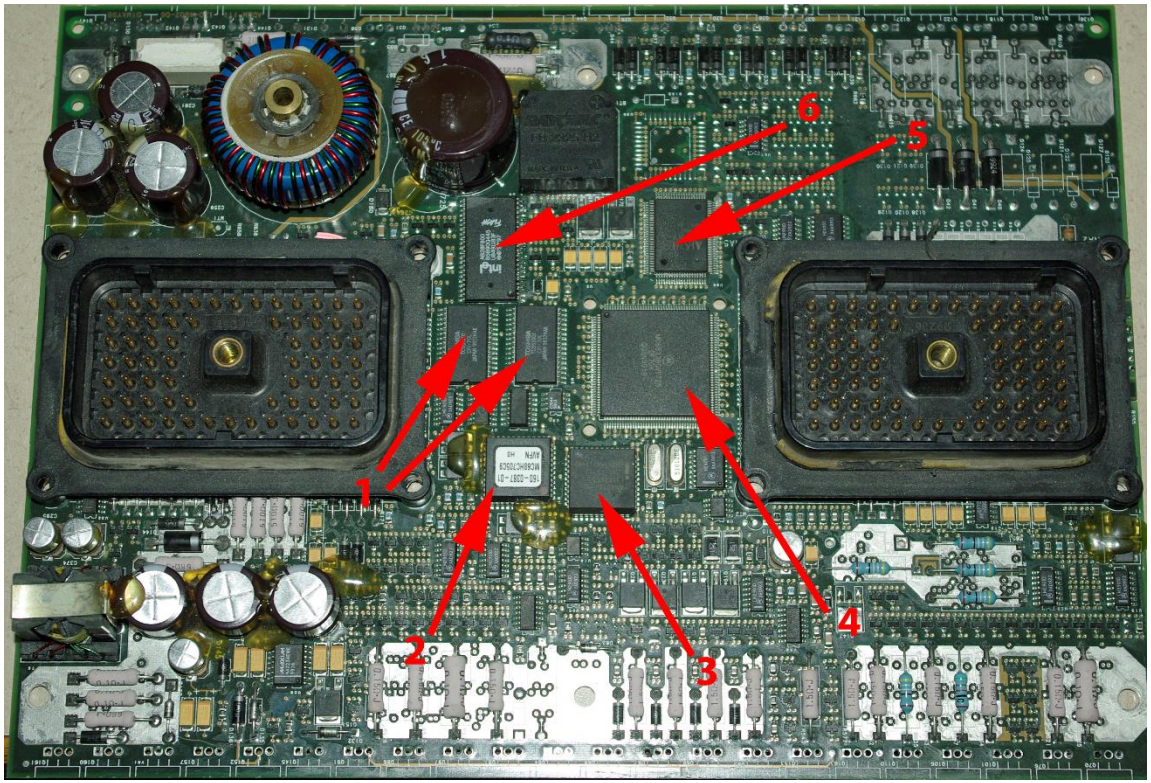
Drastic measures



Chip Identification

CAT ADEM III

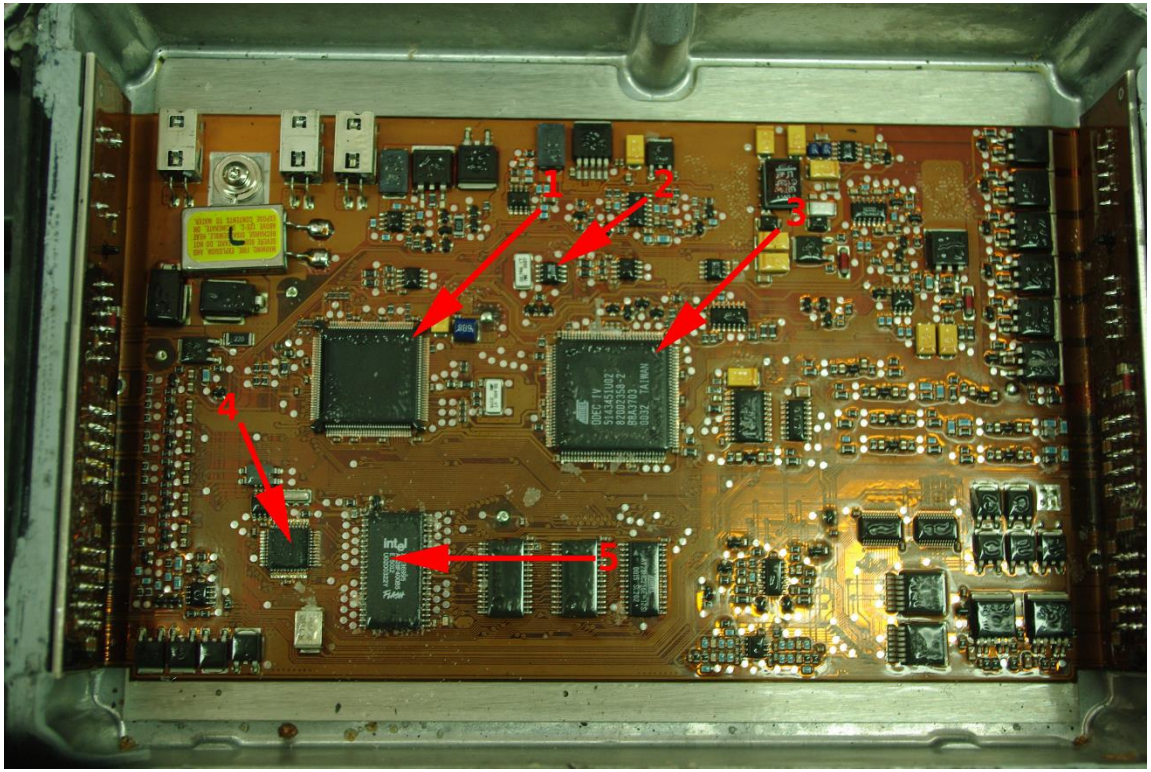
1. **Toshiba SRAM**
2. **MC68HC705C9A 8-bit Microcontroller (EEPROM)**
3. **Intel CAN 2.0 Controller**
4. **MC68336 32-bit Microprocessor (note: Mask-Rom + SRAM)**
5. **AMI IC Branded Caterpillar, Presumed ASIC**
6. **Intel AB28F800 5V Flash Storage**



Chip Identification

DDEC IV

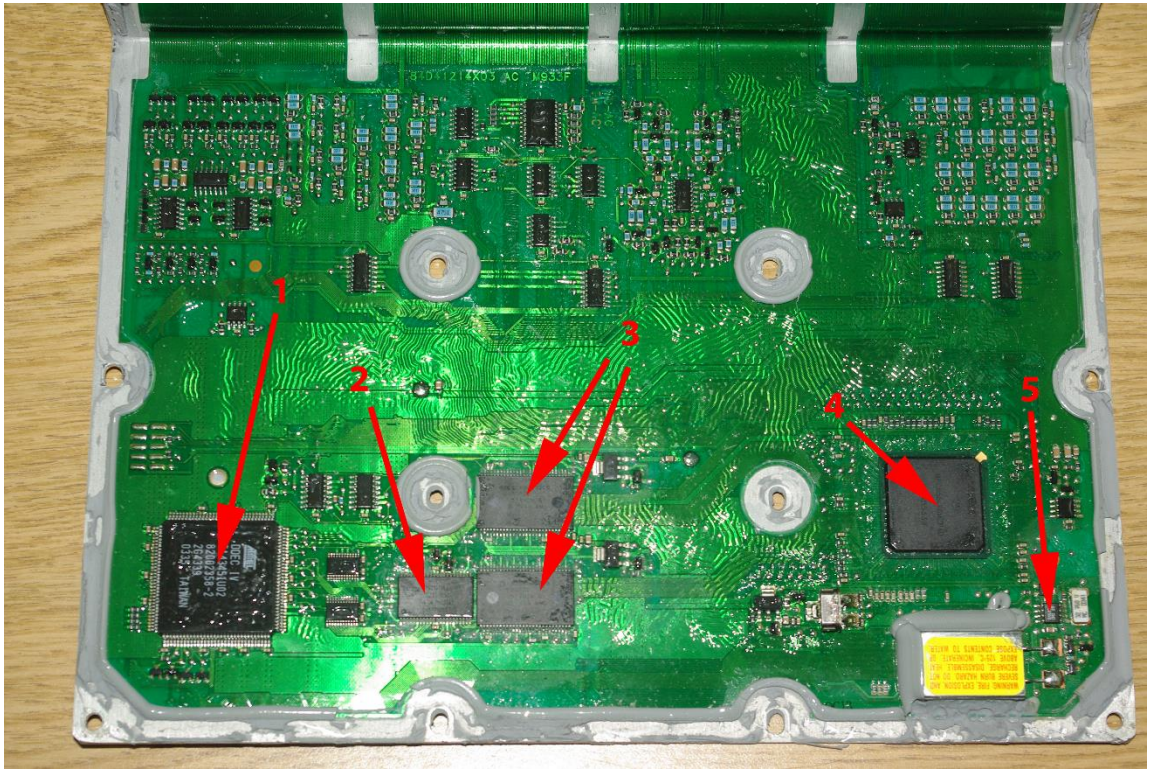
1. **MC68332 – 32-bit CPU**
2. **Real-time Clock controller**
3. **Presumed Custom ASIC controller**
4. **CAN Controller**
5. **Intel Flash Storage IC AB28F400**



Chip Identification

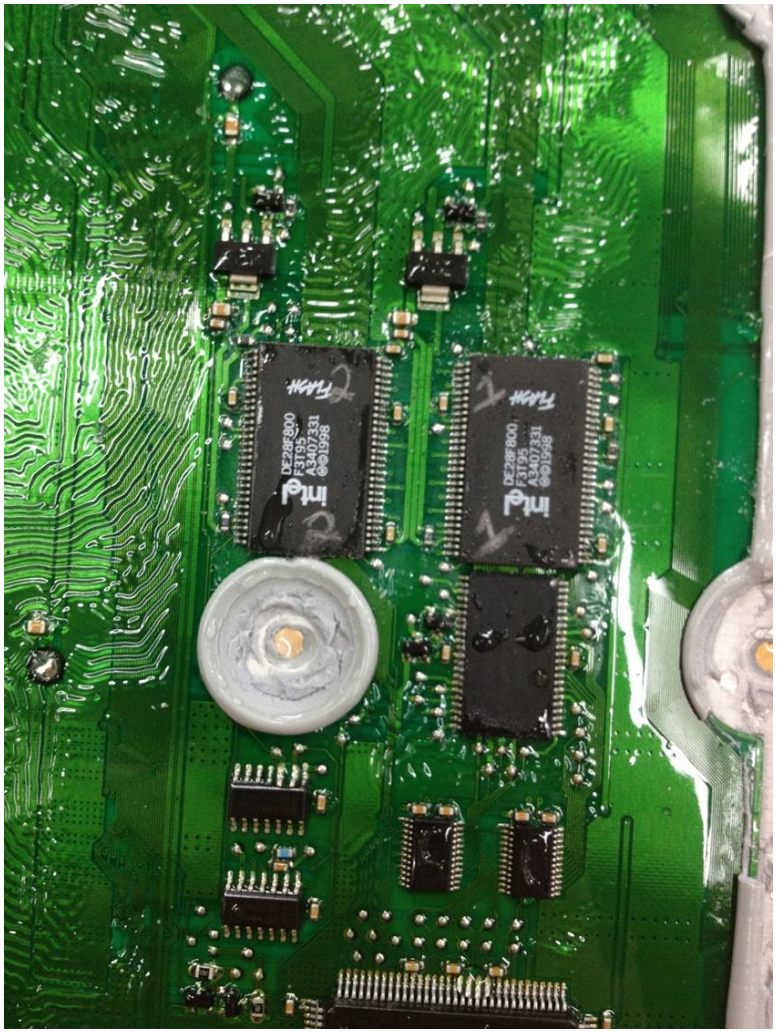
DDEC 5

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**



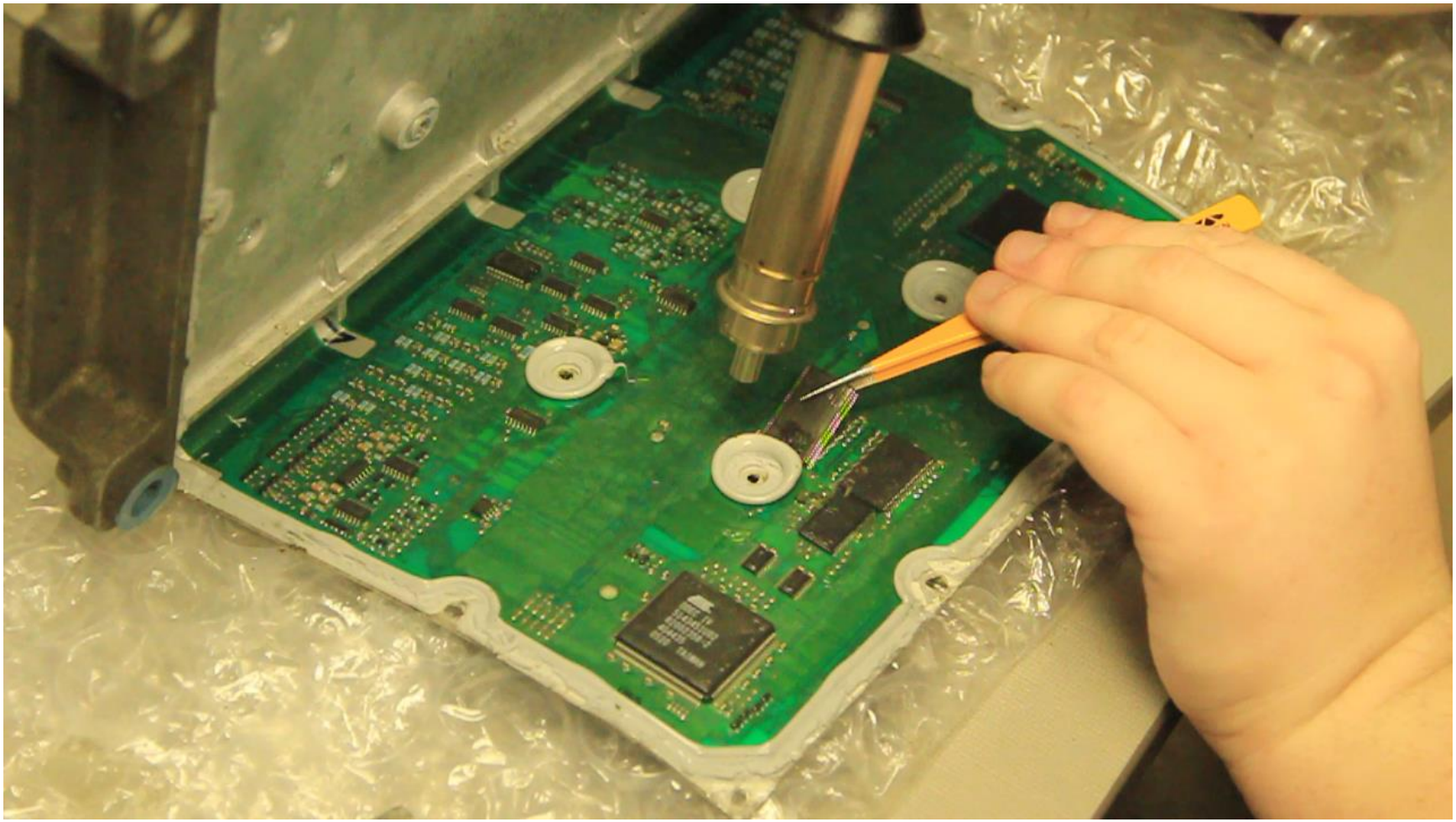
Another DDEC 5

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



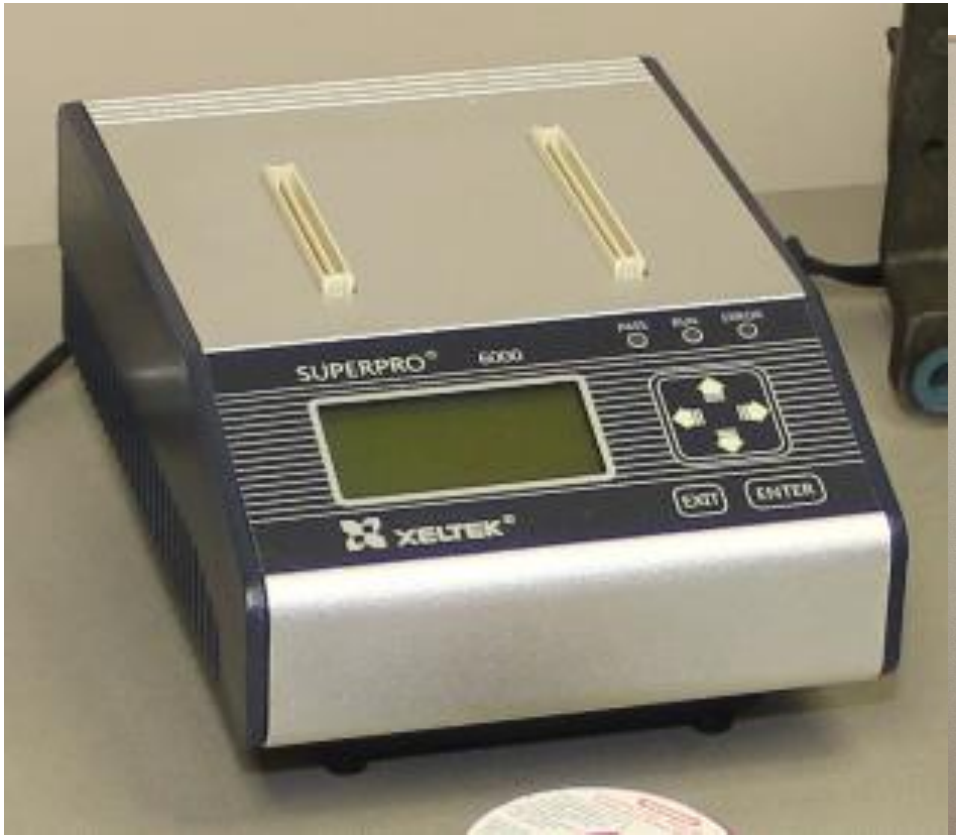
Chip Removal

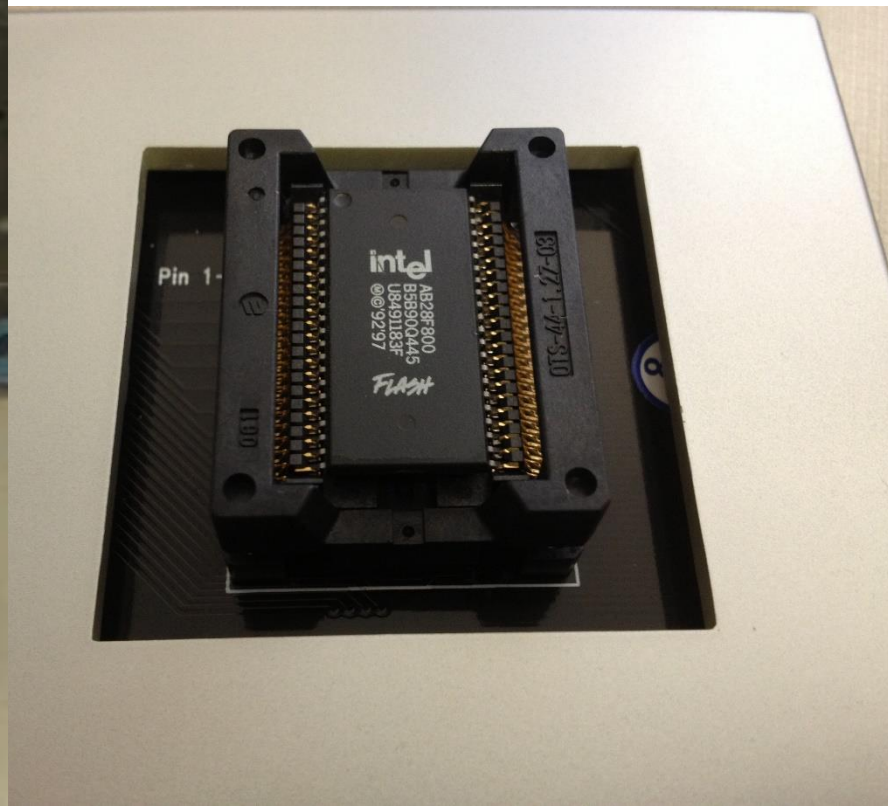
Hot air rework station to removing the flash memory



Reading the chip memory

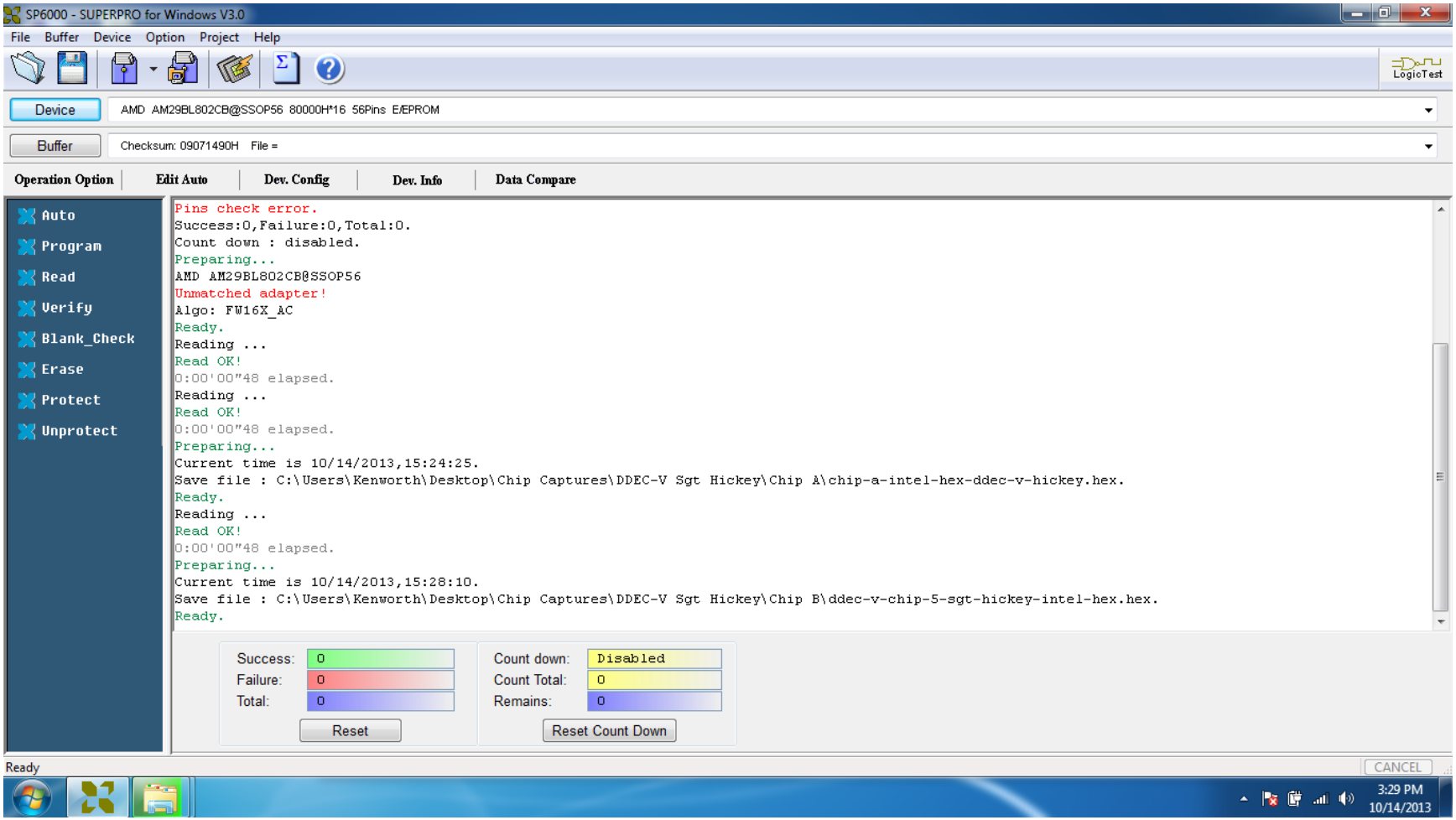
Xeltek Super Pro 6000 Universal Chip Reader



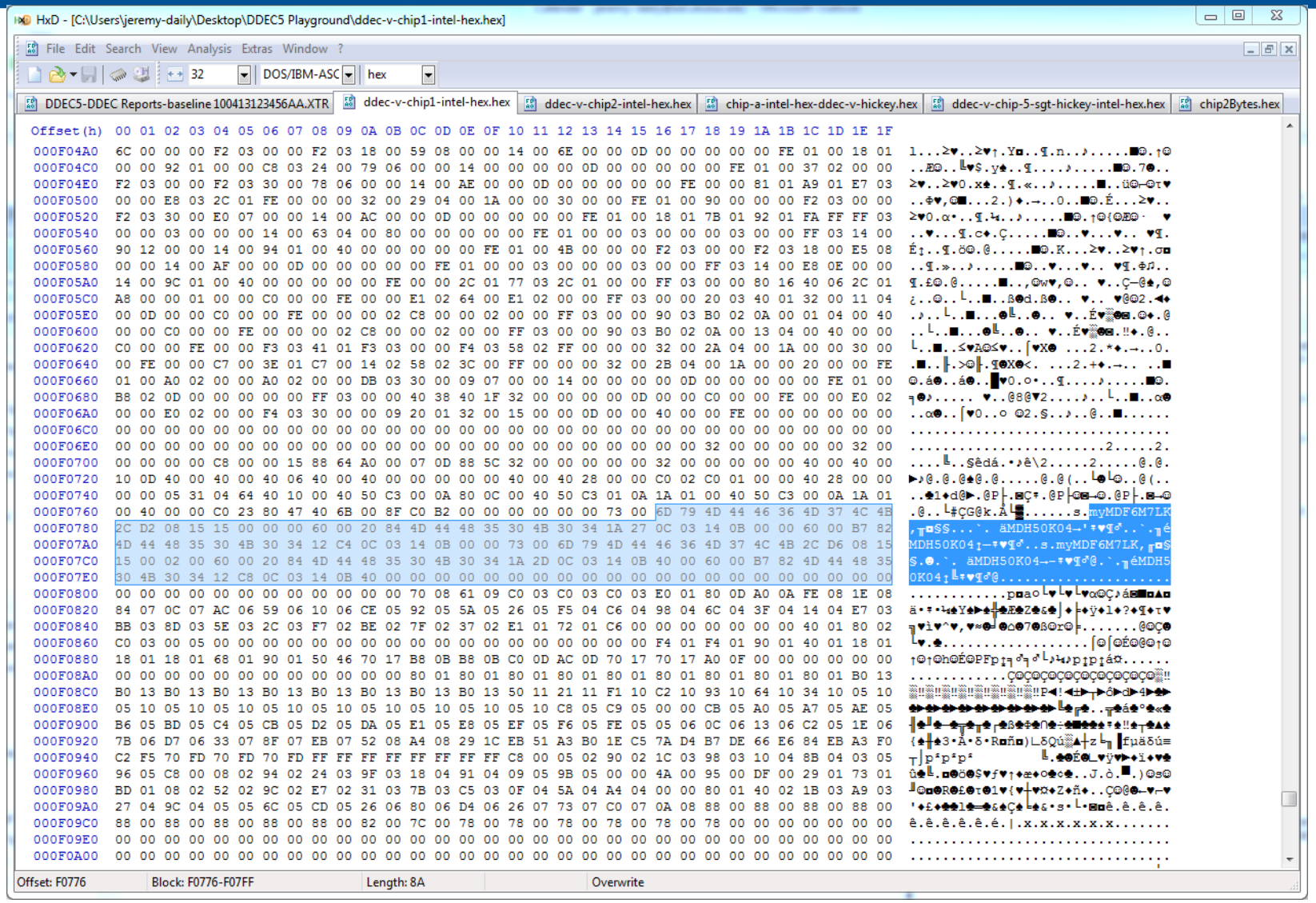


Software to run the Chip Reader

Output is a raw binary file (*.hex)



Results in a Hex editor (Now What?)



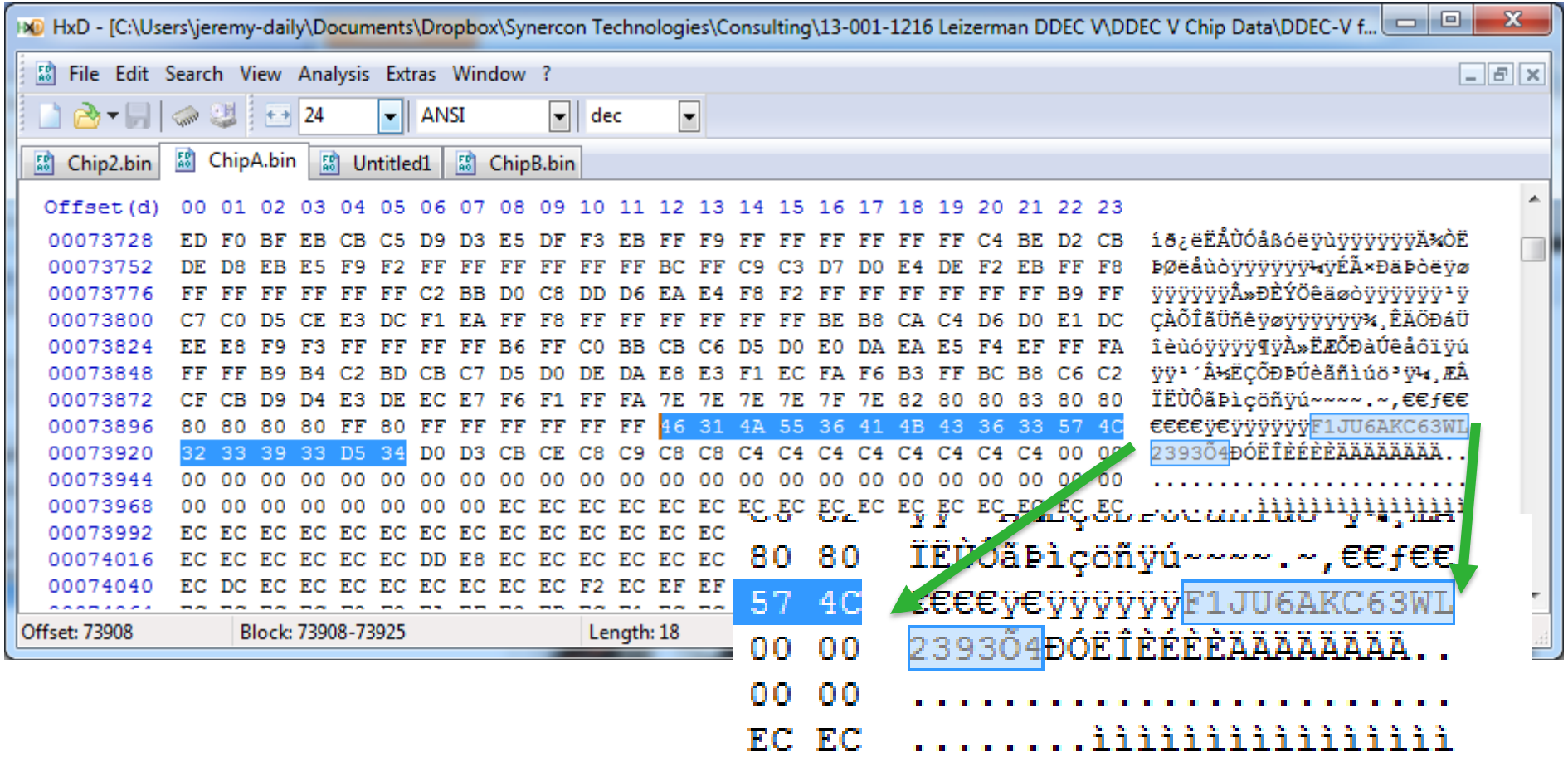
NEED TO DECODE AND INTERPRET SOME DATA

ITS ALL BINARY (HEX)!!

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”)

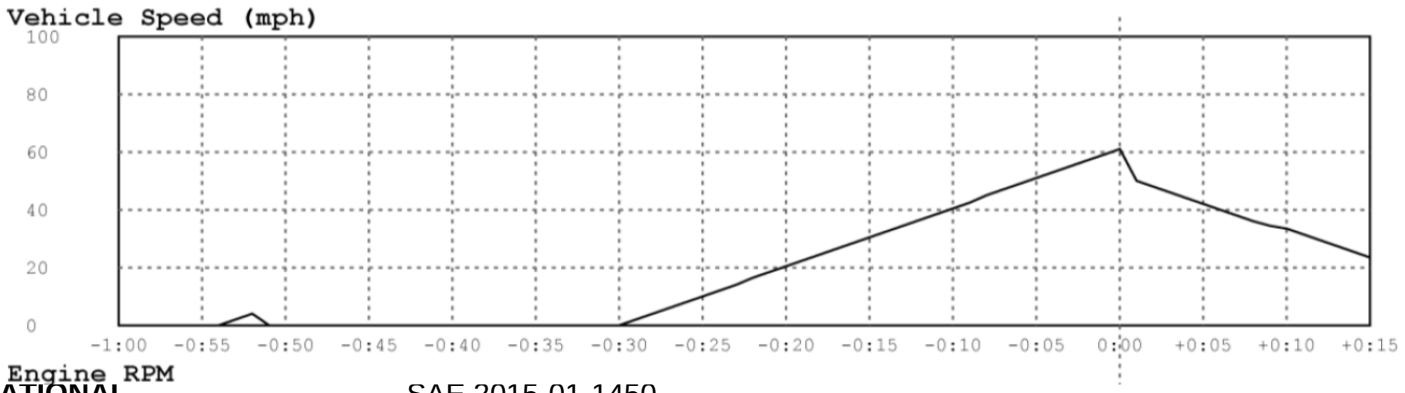
Simulated Data

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.

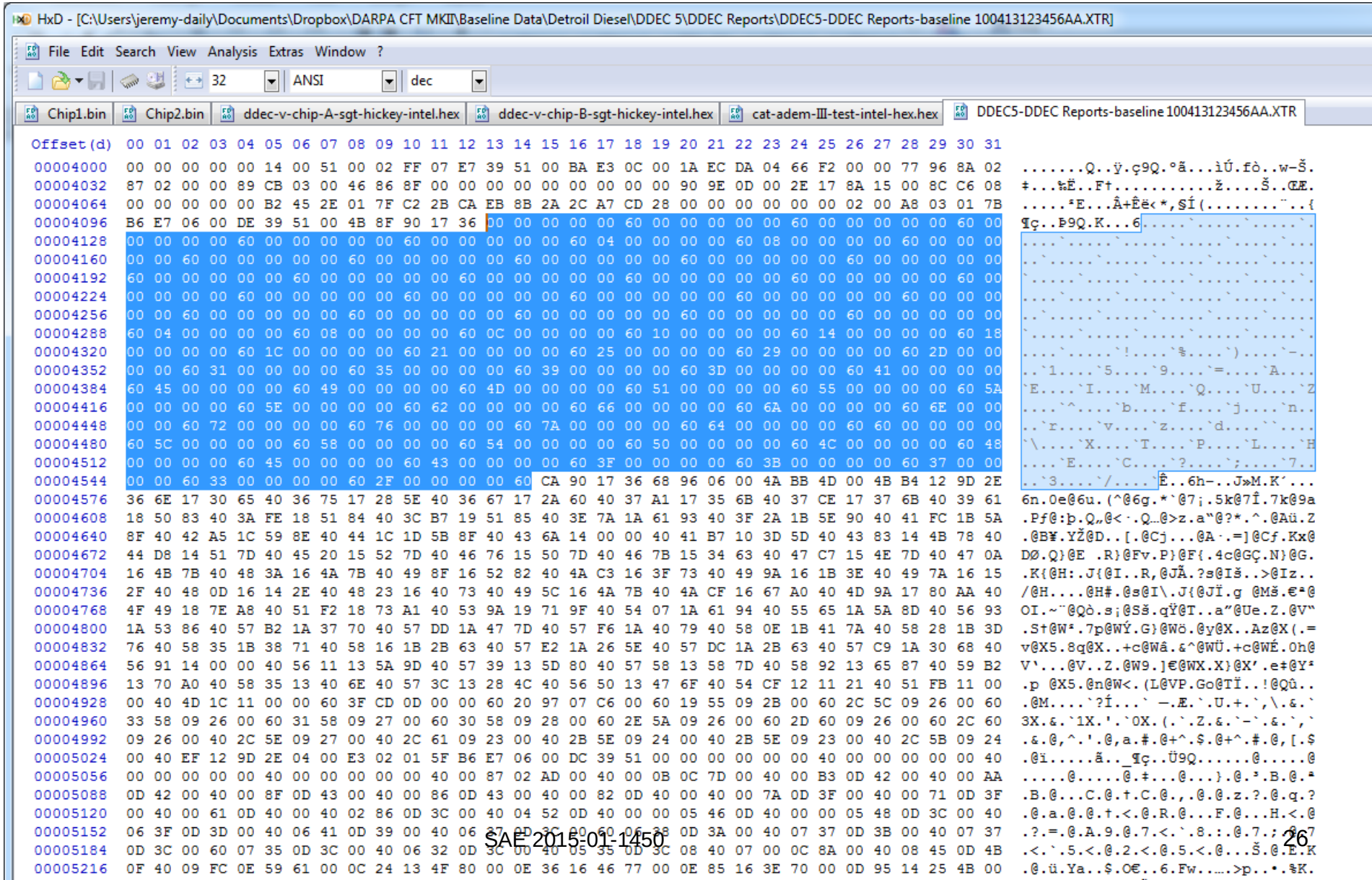
Use J1587 Transport layer to reconstruct the network traffic.

***.XTR file is close to a network log.**

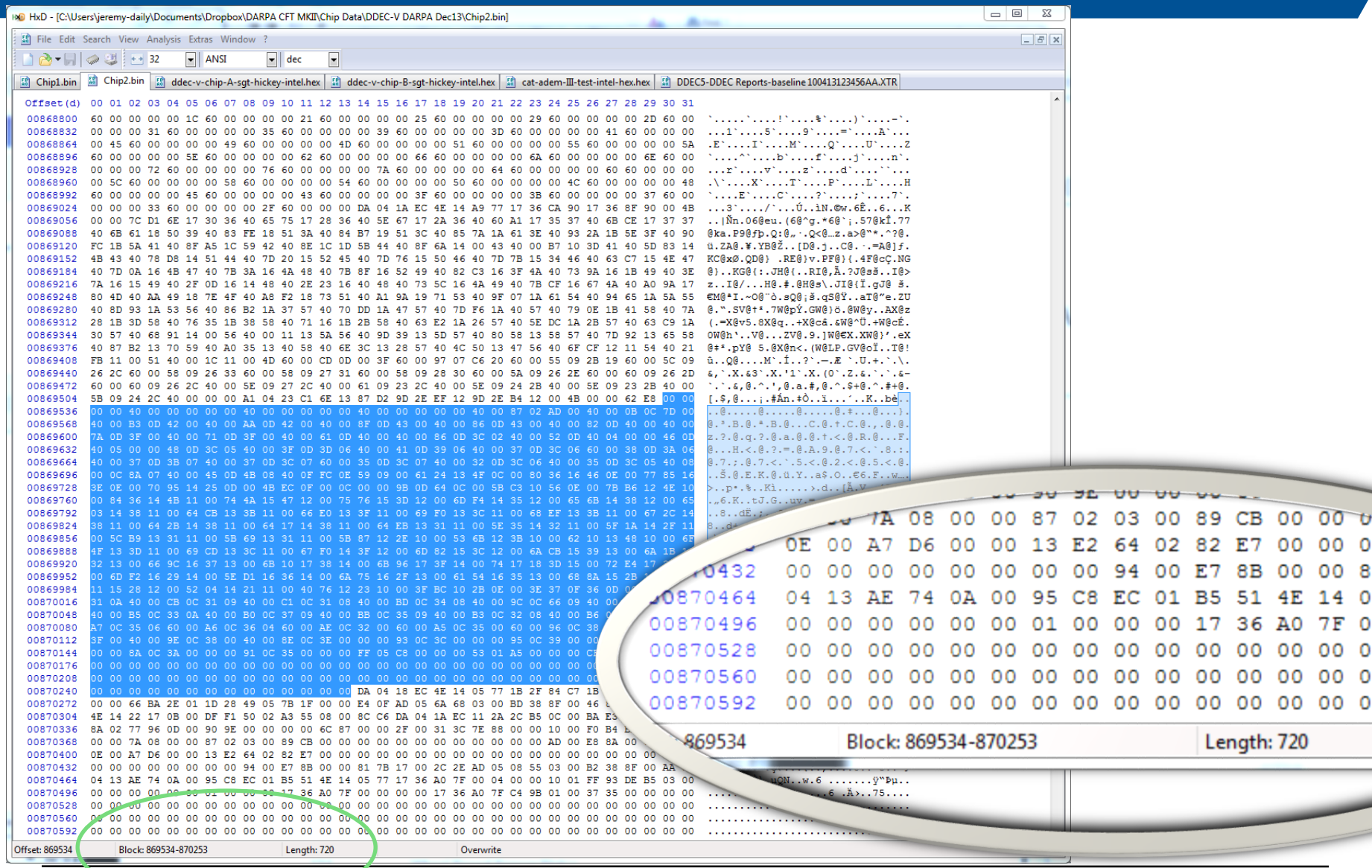
Borrowing from last year, we can map the XTR file contents to DDEC Reports elements. (2014-01-0495)

Enables pattern matching for data elements like Mileage and Times.

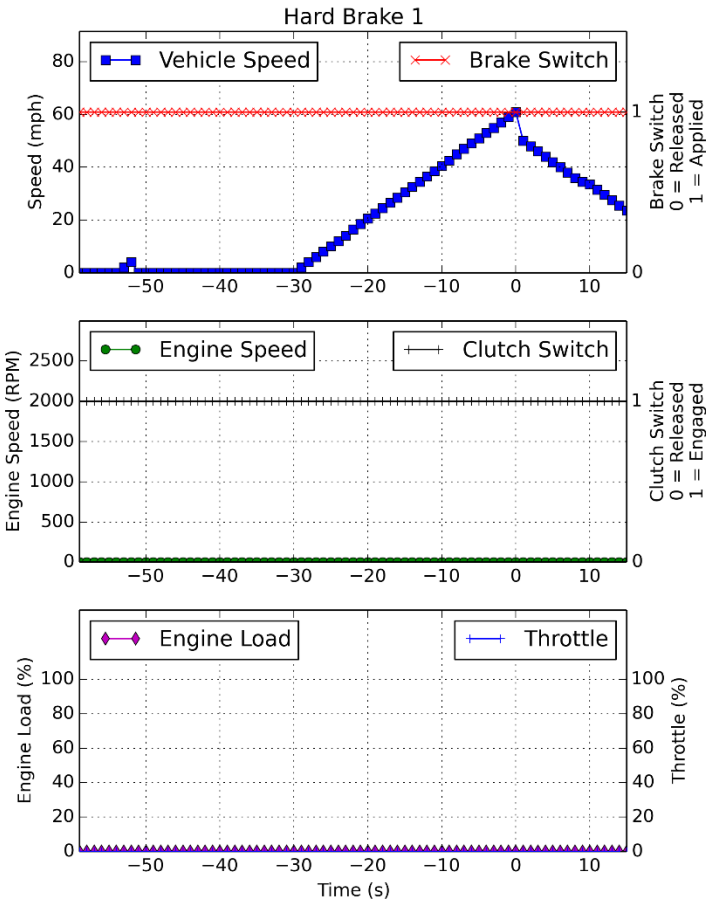
Find the Data pattern (Hard Brake)

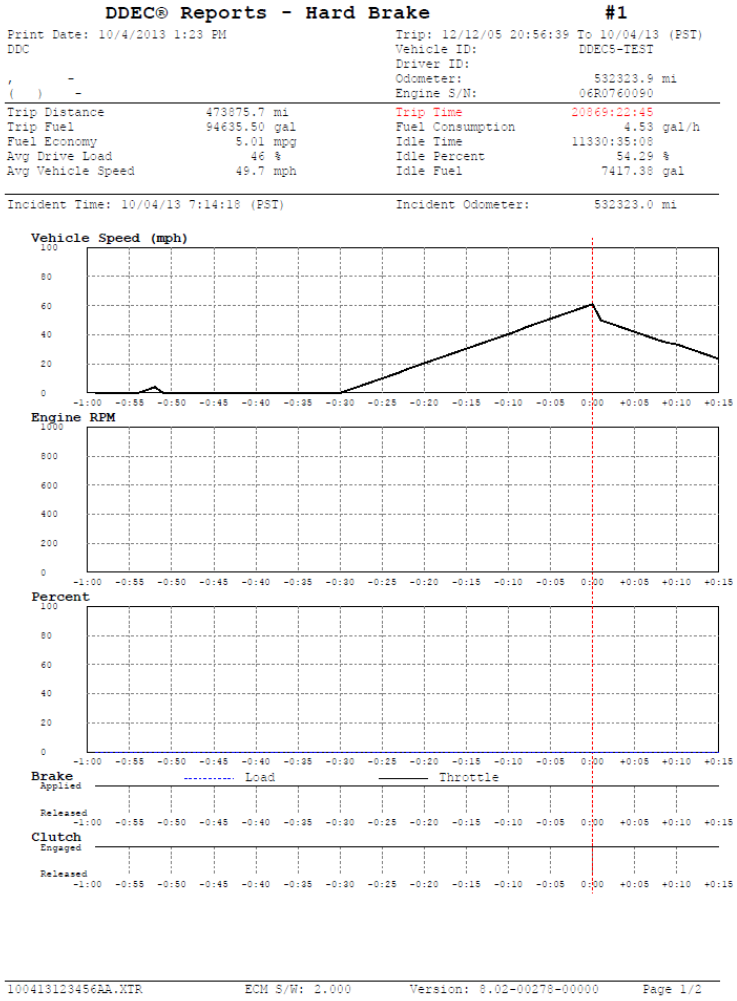


Last Stop Data



Hard Brake 1 Comparison





DDEC® Reports - Hard Brake #1

Print Date: 10/4/2013 1:23 PM
DDC

Trip: 12/12/05 20:56:39 To 10/04/13 (PST)
Vehicle ID: DDEC5-TEST
Driver ID:
Odometer: 532323.9 mi
Engine S/N: 06R0760090

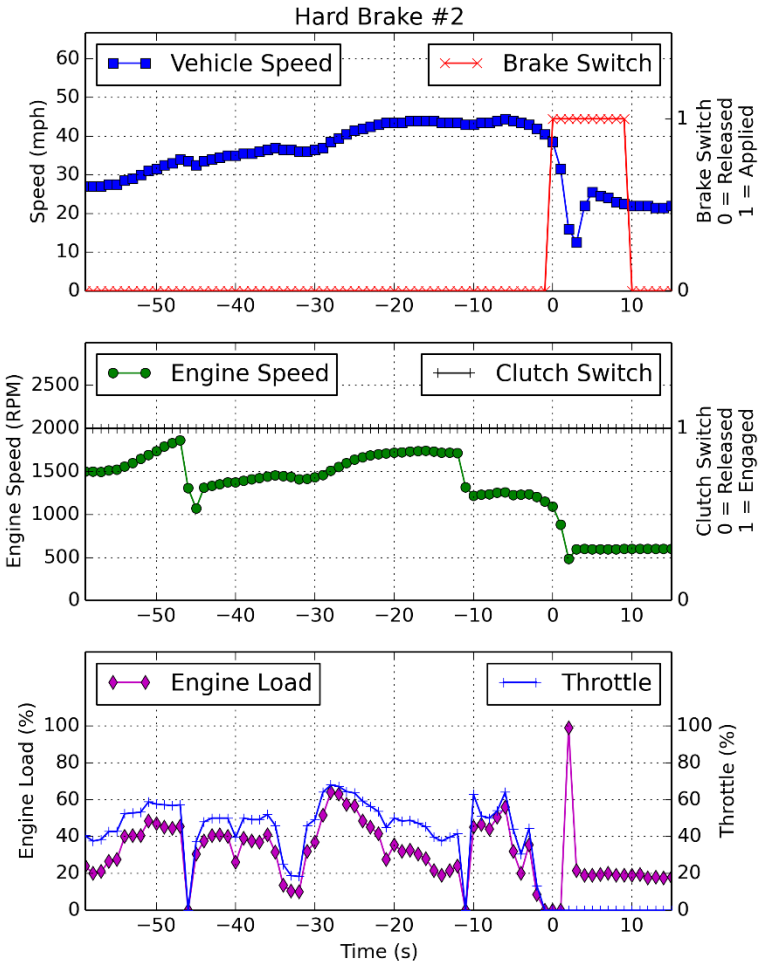
Trip Distance	473875.7 mi	Trip Time	20869:22:45
Trip Fuel	94635.50 gal	Fuel Consumption	4.53 gal/h
Fuel Economy	5.01 mpg	Idle Time	11330:35:00
Avg Drive Load	46 %	Idle Percent	54.29 %
Avg Vehicle Speed	49.7 mph	Idle Fuel	7417.38 gal

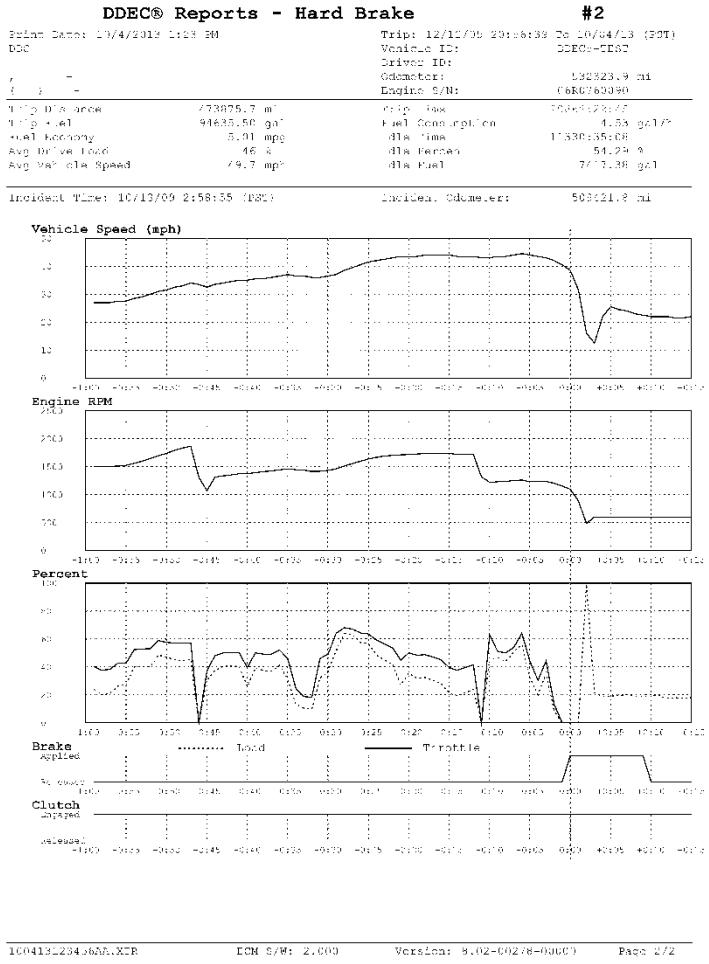
Incident Time: 10/04/13 7:14:18 (PST) Incident Odometer: 532323.0 mi

Vehicle Speed (mph)
Engine RPM
Percent
Brake Applied Released
Load
Throttle
Clutch Engaged Released

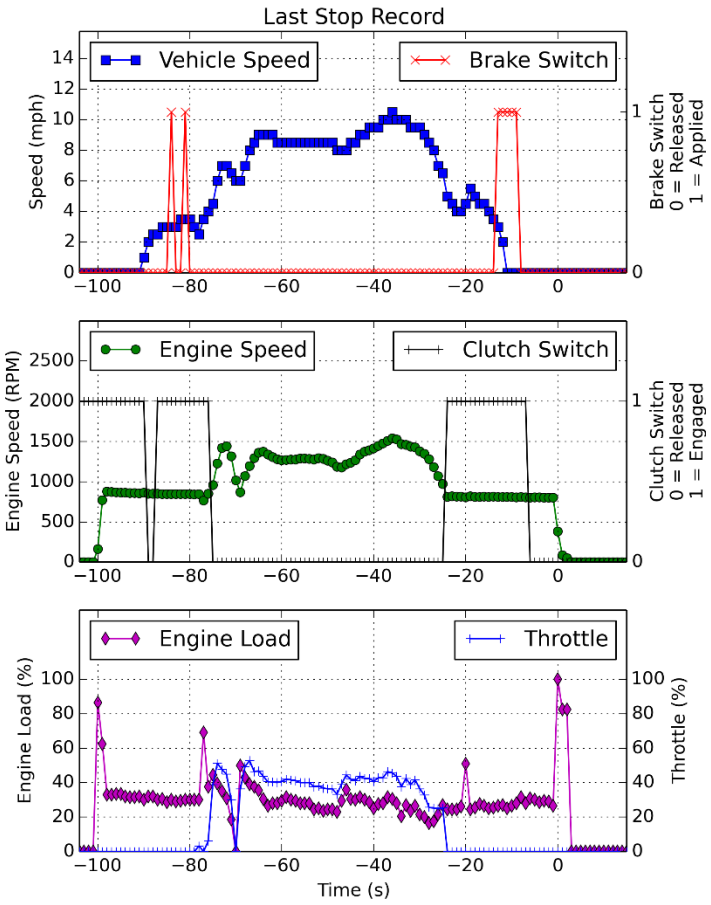
100413123456AA.XTR ECM S/W: 2.000 Version: 8.02-00278-00000 Page 1/2

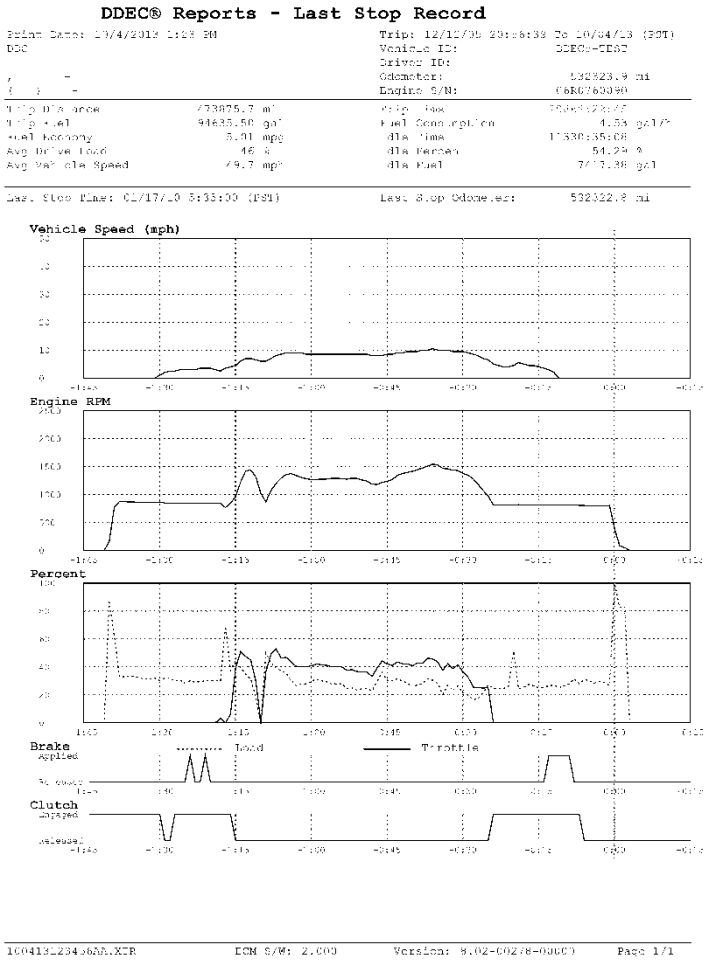
Hard Brake 2 Comparison





Last Stop Comparison





Daily Engine Usage

DDEC® Reports - Daily Engine Usage

Print Date: 8/21/2013 11:08 AM
University of Tulsa
800 S. Tucker Dr
Tulsa, OK 74104
(918)631-3056

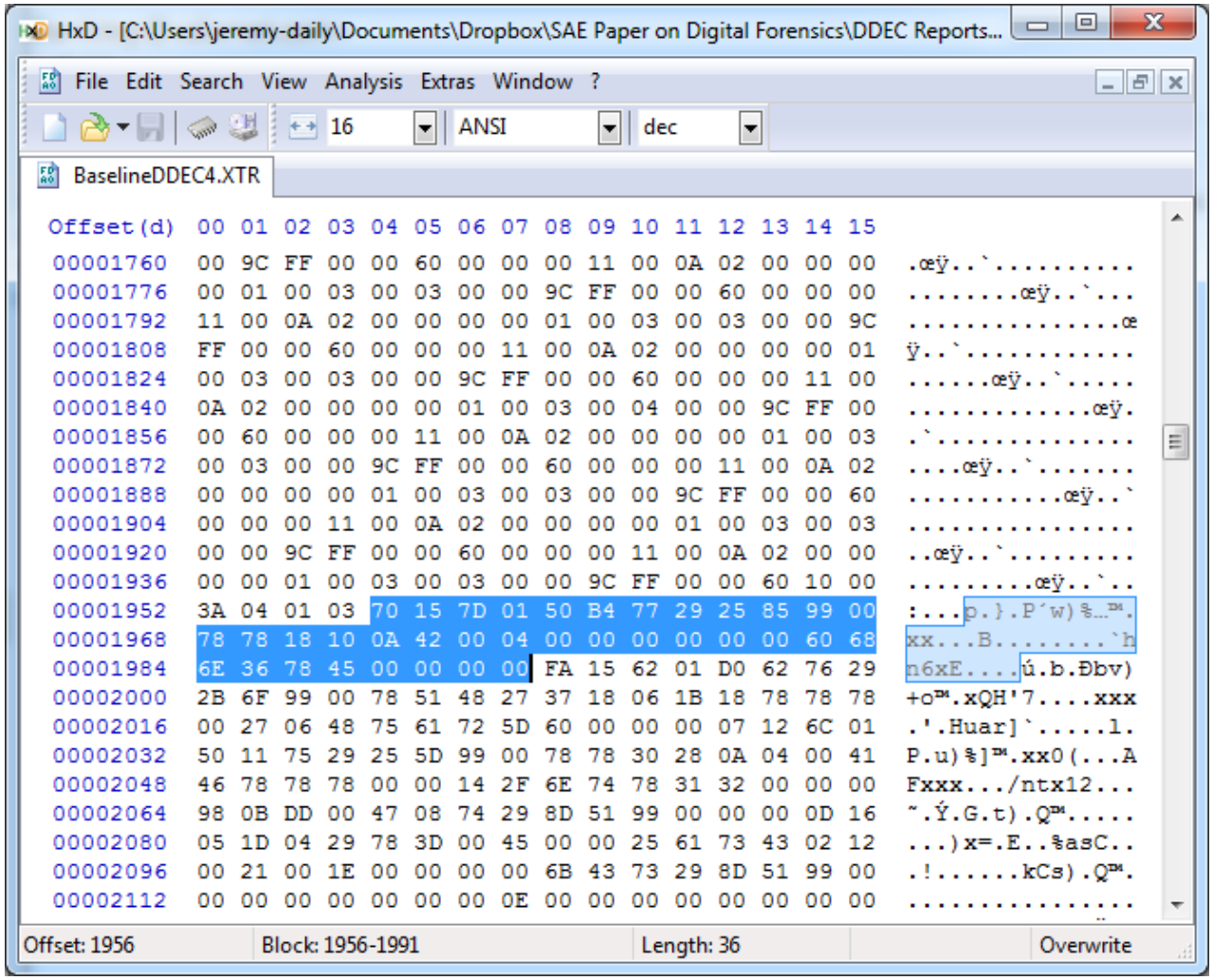
Date Range: 01/18/07 To 01/07/00 (EST)

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



Determining Data Meaning in the

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		08:00-10	
Central Standard Time		Miles	Miles	Gallons	Idle (HH:MM)	Drive (HH:MM)	Idle	Drive	Idle	Drive	Idle	Drive	Idle	Drive	Idle	D
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	00:44	1
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	00:00	1
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	116:25	0