Electronic Control Unit and CAN Data Analysis

Jeremy Daily, Ph.D., P.E.
jeremy-daily@utulsa.edu
Associate Professor of Mechanical Engineering

THE UNIVERSITY of TULSA

Student CyberTruck Experience

Overview

1. CAN Logger (version 2) Update
2. Network and Application Based CAN Capture
3. Chip Level Capture
4. Analysis, Decoding and Presenting the Data

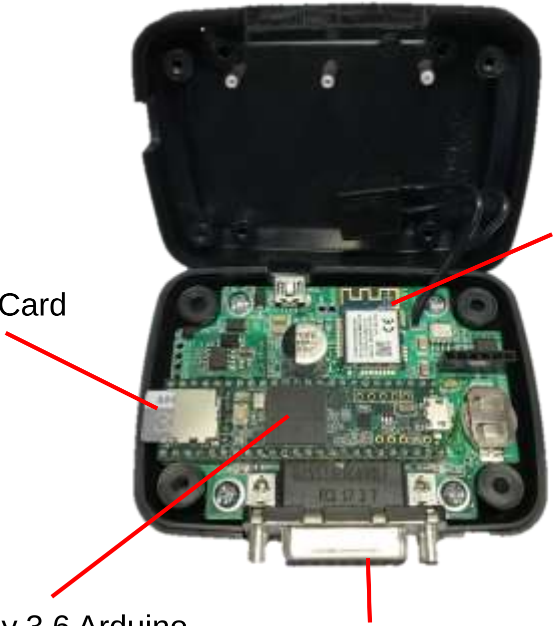
Some contents were originally published in SAE 2015-01-1450

Logging Heavy Vehicle Network Traffic

- Capture as much raw operational CAN data from heavy vehicles as possible.
  - Store Heavy Vehicle Network Messages on SD Card
  - Unique opportunity for a unique data set
  - Data is sanitized and stored by NMFTA
- Implementation
  - CAN Logger V2
  - Faster
  - More Networks
  - Better Enclosure
  - Open Source
  - Functional Tool

NMFTA CAN Logger V2

- Logging Interfaces
  - 3 – High Speed CAN
  - 1 – Single Wire CAN
  - 1 – LIN
  - 1 – J1708
- External Connectivity
  - Vehicle Network Interface
  - Wi-Fi
  - USB
- 180 MHz 32-bit ARM Cortex M4F
- Button for marking data
- Three LEDs



Wi-Fi Adapter

SD Card

Teensy 3.6 Arduino Compatible Development Board

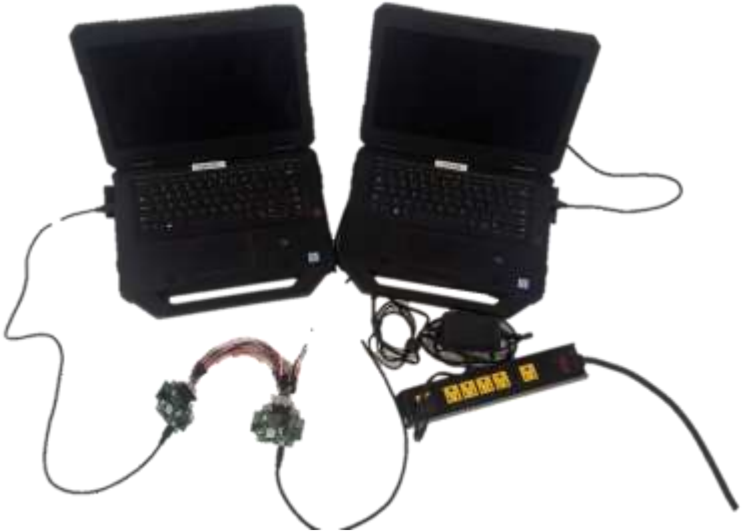
Vehicle Network Interface

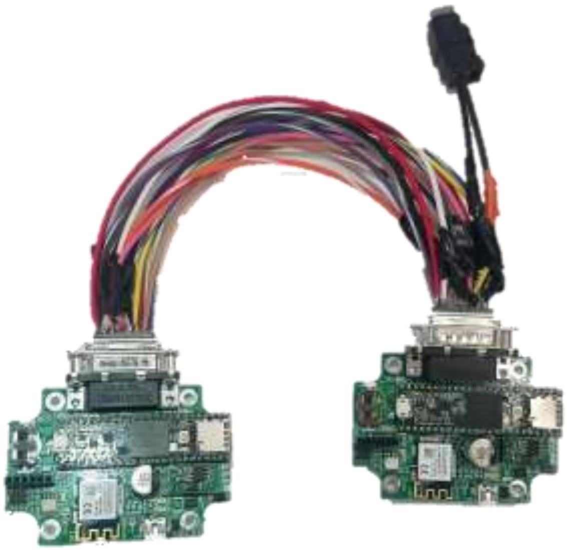
Why is it Useful?

- Vehicle Network Interface
  - D-sub 15 to Deutsch 9-Pin
  - Deutsch 9-Pin is a Heavy Vehicle Standard
  - Uses Diagnostic Port for Logging
- Easy Data Collection of Heavy Vehicle Networks
- Common Learning Platform
  - Statistical Differences Between
    - Normal Drive
    - Normal Drive with Attacks
- 100% Open Source

Deutsch 9-Pin
Connector

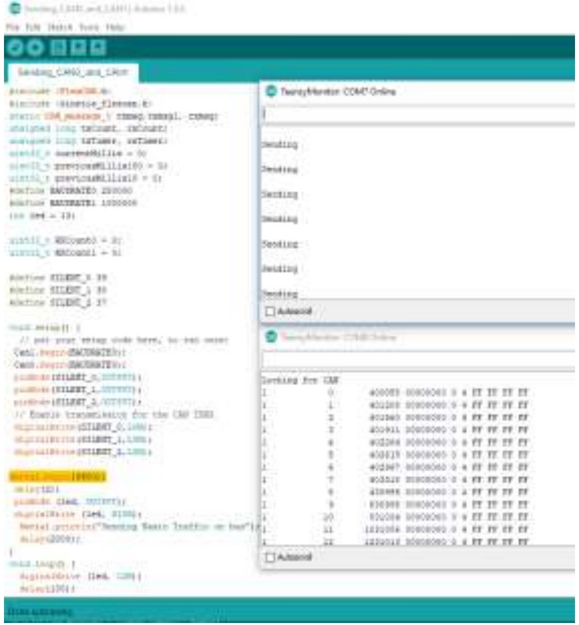
Testing: Two at a Time





Testing: Three CAN Channels

FlexCAN CAN Channels

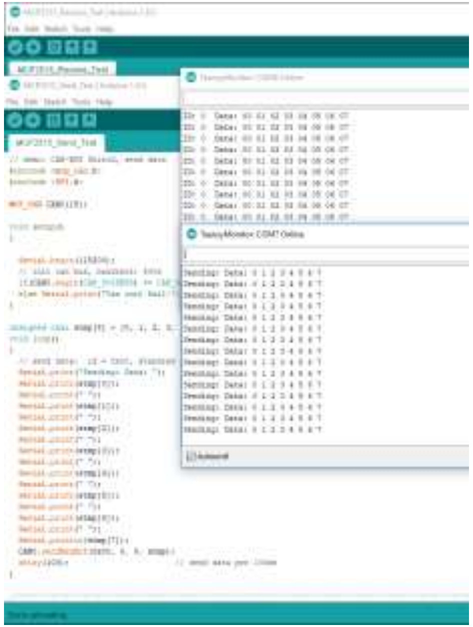

Sending_CAN0_and_CAN1 | Arduino 1.8.5
File Edit Sketch Tools Help
Sending_CAN0_and_CAN1
TeensyMonitor COM7 Online
☐ Autoscroll
TeensyMonitor COM8 Online
☐ Autoscroll
Done uploading.

```
#include <FlexCAN.h>
#include <kinetis_flexcan.h>
static CAN_message_t rxmsg, txmsg1, txmsg2;
unsigned long txCount, rxCount;
unsigned long txTimer, rxTimer;
uint32_t currentMillis = 0;
uint32_t previousMillis00 = 0;
uint32_t previousMillis0 = 0;
#define BAUDRATE0 250000
#define BAUDRATE1 1000000
int led = 13;

uint32_t RXCount0 = 0;
uint32_t RXCount1 = 0;

#define SILENT_0 39
#define SILENT_1 38
#define SILENT_2 37

void setup() {
  // put your setup code here, to run once:
 Can0.begin(BAUDRATE0);
 Can1.begin(BAUDRATE1);
 pinMode(SILENT_0,OUTPUT);
 pinMode(SILENT_1,OUTPUT);
 pinMode(SILENT_2,OUTPUT);
 // Enable transmission for the CAN [illegible]
 digitalWrite(SILENT_0,LOW);
 digitalWrite(SILENT_1,LOW);
 digitalWrite(SILENT_2,LOW);

Serial.begin(9600);
 delay(10);
 pinMode (led, OUTPUT);
 digitalWrite (led, HIGH);
  Serial.println("Sending Basic Traffic on bus");
  delay(2000);
}
void loop() {
  digitalWrite (led, LOW);
  delay(100);
```

```
Sending

Sending

Sending

Sending

Sending

Sending

Sending
```

```
Looking for CAN
1          0       400085 00000000 0 4 FF FF FF FF
1          1       402100 00000000 0 4 FF FF FF FF
1          2       402960 00000000 0 4 FF FF FF FF
1          3       401911 00000000 0 4 FF FF FF FF
1          4       402288 00000000 0 4 FF FF FF FF
1          5       403015 00000000 0 4 FF FF FF FF
1          6       402867 00000000 0 4 FF FF FF FF
1          7       403520 00000000 0 4 FF FF FF FF
1          8       410444 00000000 0 4 FF FF FF FF
1          9       810388 00000000 0 4 FF FF FF FF
1         10       832084 00000000 0 4 FF FF FF FF
1         11      1232084 00000000 0 4 FF FF FF FF
1         12      1232012 00000000 0 4 FF FF FF FF
```

MCP 2515 CAN Channel


MCP2515_Receive_Test | Arduino 1.8.5
File Edit Sketch Tools Help
MCP2515_Receive_Test
MCP2515_Send_Test | Arduino 1.8.5
File Edit Sketch Tools Help
MCP2515_Send_Test
TeensyMonitor COM8 Online
TeensyMonitor COM7 Online
☐ Autoscroll
Done uploading.

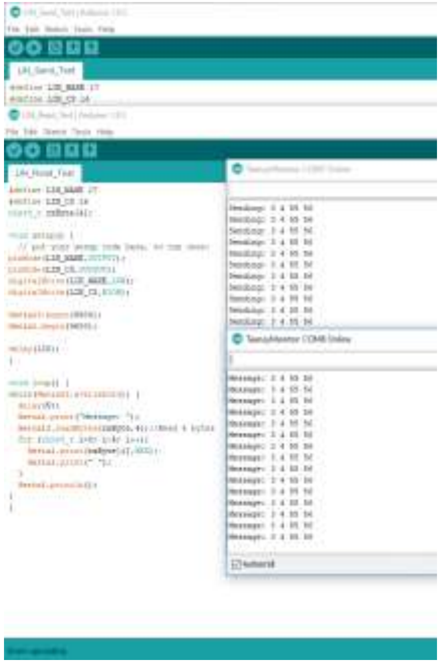
```
// demo: CAN-BUS Shield, send data
#include <mcp_can.h>
#include <SPI.h>

MCP_CAN CAN0(10);

void setup()
{
  Serial.begin(115200);
  // init can bus, baudrate: 500k
  if(CAN0.begin(CAN_500KBPS) == CAN_OK) [illegible]
  else Serial.print("Can init fail!!\r\n");
}

unsigned char stmp[8] = {0, 1, 2, 3, [illegible]
void loop()
{
  // send data:  id = 0x00, standard [illegible]
  Serial.print("Sending: Data: ");
  Serial.print(stmp[0]);
  Serial.print(" ");
  Serial.print(stmp[1]);
  Serial.print(" ");
  Serial.print(stmp[2]);
  Serial.print(" ");
  Serial.print(stmp[3]);
  Serial.print(" ");
  Serial.print(stmp[4]);
  Serial.print(" ");
  Serial.print(stmp[5]);
  Serial.print(" ");
  Serial.print(stmp[6]);
  Serial.print(" ");
  Serial.println(stmp[7]);
  CAN0.sendMsgBuf(0x00, 0, 8, stmp);
  delay(100);                       // send data per 100ms
}
```

```
ID: 0  Data: 00 01 02 03 04 05 06 07
ID: 0  Data: 00 01 02 03 04 05 06 07
ID: 0  Data: 00 01 02 03 04 05 06 07
ID: 0  Data: 00 01 02 03 04 05 06 07
ID: 0  Data: 00 01 02 03 04 05 06 07
ID: 0  Data: 00 01 02 03 04 05 06 07
ID: 0  Data: 00 01 02 03 04 05 06 07
ID: 0  Data: 00 01 02 03 04 05 06 07
ID: 0  Data: 00 01 02 03 04 05 06 07
ID: 0  Data: 00 01 02 03 04 05 06 07
```

```
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
Sending: Data: 0 1 2 3 4 5 6 7
```

Testing: Other Vehicle Networks

LIN


LIN_Send_Test | Arduino 1.8.x
File Edit Sketch Tools Help
LIN_Send_Test
LIN_Read_Test | Arduino 1.8.x
File Edit Sketch Tools Help
LIN_Read_Test
TeensyMonitor COM8 Online
Autoscroll
Done uploading.

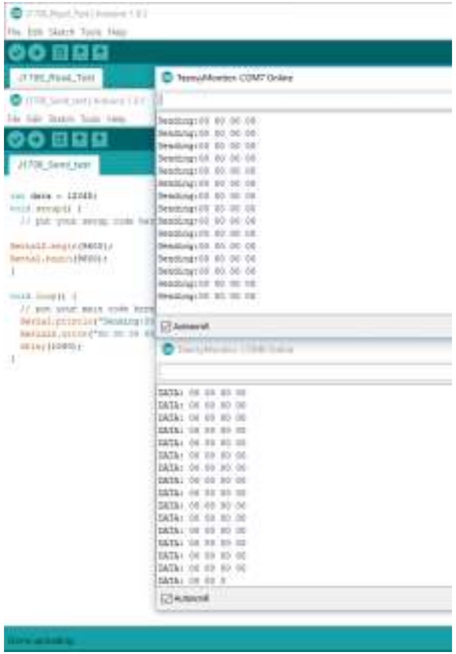
```
#define LIN_WAKE 17
#define LIN_CS 16
```

```
#define LIN_WAKE 17
#define LIN_CS 16
uint8_t rxBytes[4];

void setup() {
  // put your setup code here, to run once:
pinMode(LIN_WAKE,OUTPUT);
pinMode(LIN_CS,OUTPUT);
digitalWrite(LIN_WAKE,LOW);
digitalWrite(LIN_CS,HIGH);

Serial1.begin(9600);
Serial.begin(9600);

delay(100);
}

void loop() {
while(Serial1.available()) {
  delay(5);
  Serial.print("Message: ");
  Serial1.readBytes(rxBytes,4);//Read 4 bytes
  for (uint8_t i=0; i<4; i++){
    Serial.print(rxBytes[i],HEX);
    Serial.print(" ");
  }
  Serial.println();
}
}
```

```
Sending: 3 4 55 56
Sending: 3 4 55 56
Sending: 3 4 55 56
Sending: 3 4 55 56
Sending: 3 4 55 56
Sending: 3 4 55 56
Sending: 3 4 55 56
Sending: 3 4 55 56
Sending: 3 4 55 56
Sending: 3 4 55 56
Sending: 3 4 55 56
```

```
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
Message: 3 4 55 56
```

J1708


J1708_Read_Test | Arduino 1.8.x
File Edit Sketch Tools Help
J1708_Read_Test
J1708_Send_test | Arduino 1.8.x
File Edit Sketch Tools Help
J1708_Send_test
TeensyMonitor COM7 Online
Autoscroll
TeensyMonitor COM8 Online
Autoscroll
Done uploading.

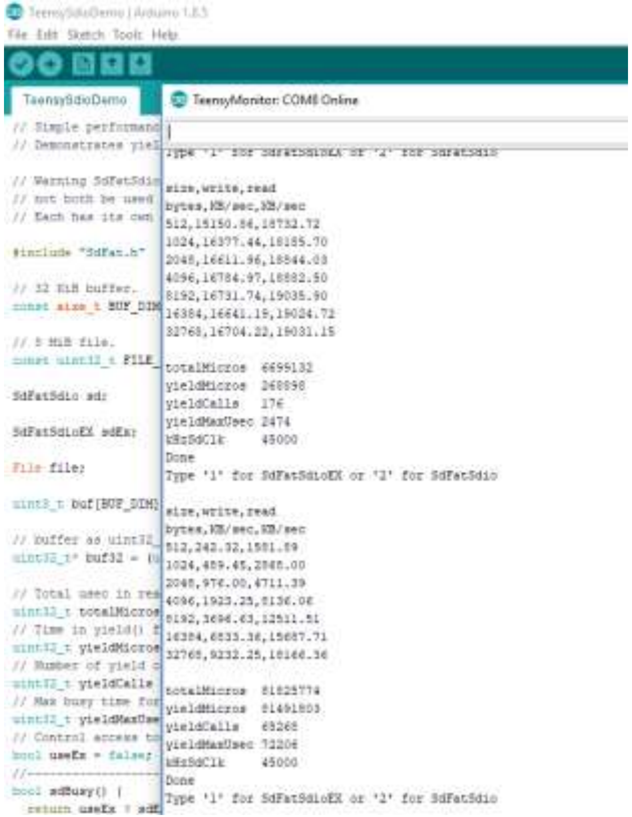
```
int data = 12345;
void setup() {
  // put your setup code her

Serial2.begin(9600);
Serial.begin(9600);
}

void loop() {
  // put your main code here
  Serial.println("Sending:00
  Serial2.print("00 80 00 0
  delay(1000);
}
```

```
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
Sending:00 80 00 08
```

```
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 80 00
DATA: 08 00 8
```

Testing: SD Card Writing Speed

- Write Time
  - 512 Bytes ≈ 240μS
- Suitable For:
  - Full Bus Loads
  - Multiple CAN Channels
  - Logging Secondary Communications


TeensySdioDemo | Arduino 1.8.5
File Edit Sketch Tools Help
TeensySdioDemo
TeensyMonitor: COM8 Online

```
// Simple performanc
// Demonstrates yiel

// Warning SdFatSdio
// not both be used
// Each has its own

#include "SdFat.h"

// 32 KiB buffer.
const size_t BUF_DIM

// 5 MiB file.
const uint32_t FILE_

SdFatSdio sd;

SdFatSdioEX sdEx;

File file;

uint8_t buf[BUF_DIM]

// buffer as uint32_
uint32_t* buf32 = (u

// Total usec in rea
uint32_t totalMicros
// Time in yield() f
uint32_t yieldMicros
// Number of yield c
uint32_t yieldCalls
// Max busy time for
uint32_t yieldMaxUse
// Control access to
bool useEx = false;
//-------------------
bool sdBusy() {
  return useEx ? sdE
```

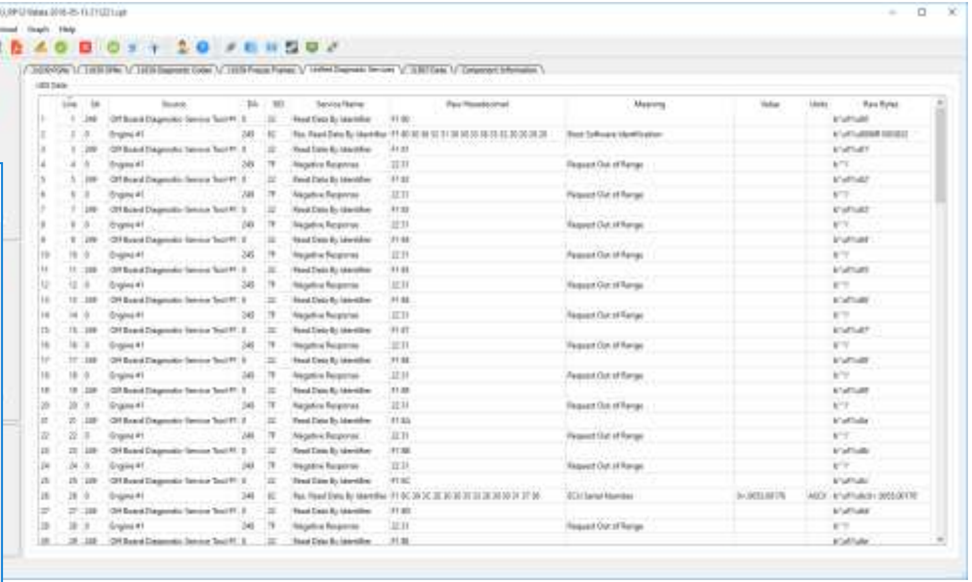
```
Type '1' for SdFatSdioEX or '2' for SdFatSdio

size,write,read
bytes,KB/sec,KB/sec
512,15150.86,18732.72
1024,16377.44,18185.70
2048,16611.96,18544.03
4096,16784.97,18882.50
8192,16731.74,19035.90
16384,16641.19,19024.72
32768,16704.22,19031.15

totalMicros  6699132
yieldMicros  268898
yieldCalls   176
yieldMaxUsec 2474
kHzSdClk     45000
Done
Type '1' for SdFatSdioEX or '2' for SdFatSdio

size,write,read
bytes,KB/sec,KB/sec
512,242.32,1581.89
1024,489.45,2848.00
2048,976.00,4711.39
4096,1923.25,8136.06
8192,3696.63,12511.51
16384,6833.36,15687.71
32768,9232.25,18166.36

totalMicros  81825774
yieldMicros  81491803
yieldCalls   65268
yieldMaxUsec 72206
kHzSdClk     45000
Done
Type '1' for SdFatSdioEX or '2' for SdFatSdio
```

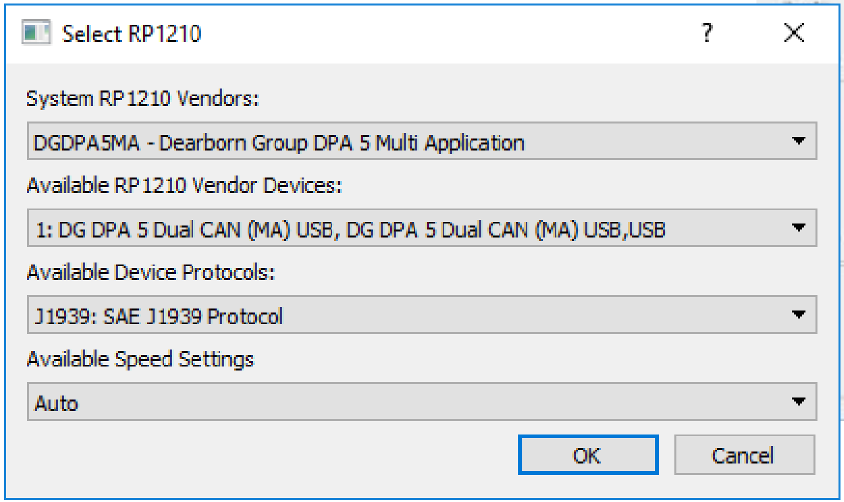
Alternative Method of Acquiring Data:

LOGGING DATA WITH RP1210 APPLICATIONS

The TU-RP1210 Application

- A Graphical User Interface to log, decode, and display data in with an open framework.
- Python, Qt, and ctypes
  - Uses DLLs from RP1210 Vendors





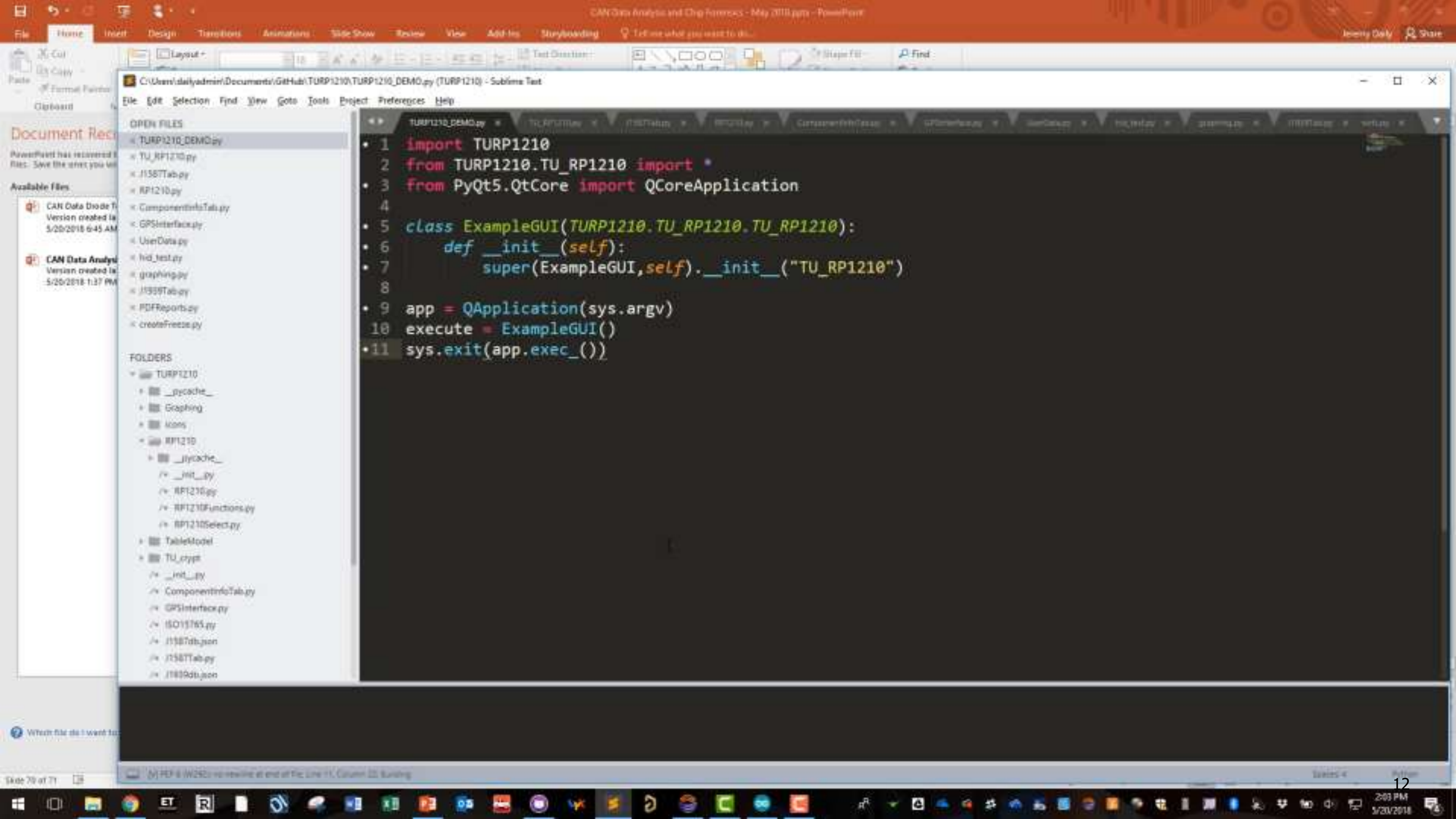
Select RP1210

System RP1210 Vendors: DGDPA5MA - Dearborn Group DPA 5 Multi Application

Available RP1210 Vendor Devices: 1: DG DPA 5 Dual CAN (MA) USB, DG DPA 5 Dual CAN (MA) USB,USB

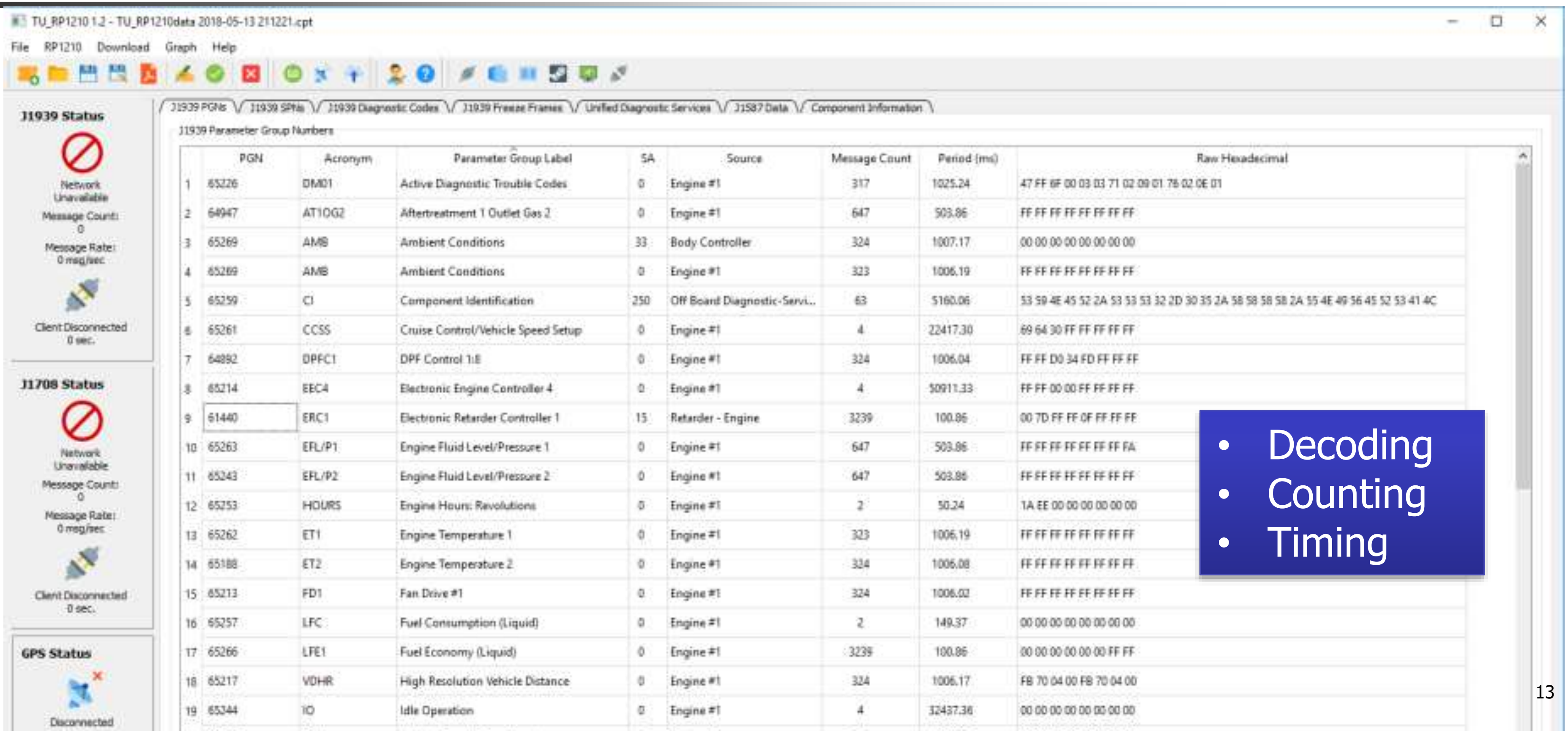
Available Device Protocols: J1939: SAE J1939 Protocol

Available Speed Settings: Auto



```
import TURP1210
from TURP1210.TU_RP1210 import *
from PyQt5.QtCore import QCoreApplication

class ExampleGUI(TURP1210.TU_RP1210.TU_RP1210):
    def __init__(self):
        super(ExampleGUI,self).__init__("TU_RP1210")

app = QApplication(sys.argv)
execute = ExampleGUI()
sys.exit(app.exec_())
```

J1939 Parameter Group Numbers



J1939 Status
Network Unavailable
Message Count: 0
Message Rate: 0 msg/sec
Client Disconnected 0 sec.

J1708 Status
Network Unavailable
Message Count: 0
Message Rate: 0 msg/sec
Client Disconnected 0 sec.

GPS Status
Disconnected

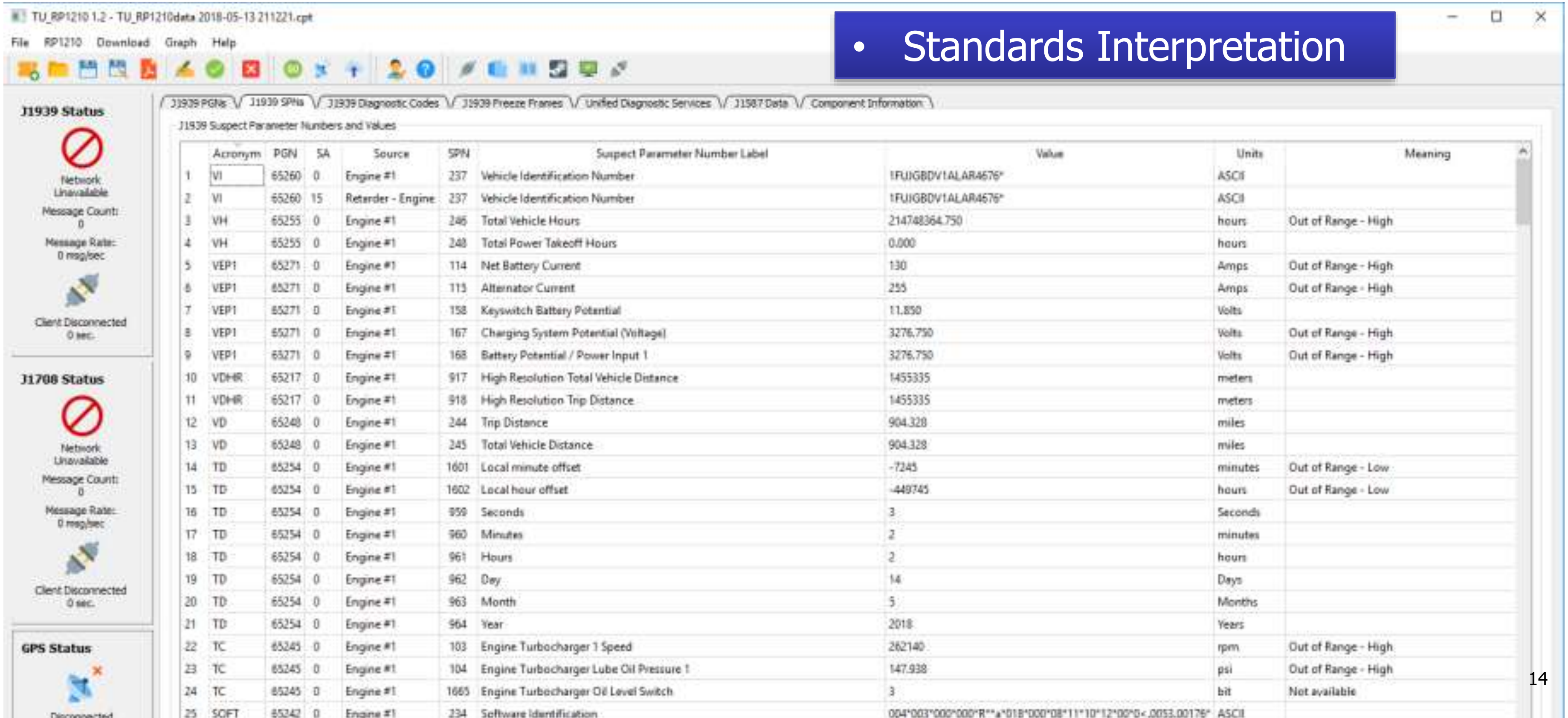
J1939 Parameter Group Numbers

	PGN	Acronym	Parameter Group Label	SA	Source	Message Count	Period (ms)	Raw Hexadecimal
1	65226	DM01	Active Diagnostic Trouble Codes	0	Engine #1	317	1025.24	47 FF 6F 00 03 03 71 02 09 01 76 02 0E 01
2	64947	AT1OG2	Aftertreatment 1 Outlet Gas 2	0	Engine #1	647	503.86	FF FF FF FF FF FF FF FF
3	65269	AMB	Ambient Conditions	33	Body Controller	324	1007.17	00 00 00 00 00 00 00 00
4	65269	AMB	Ambient Conditions	0	Engine #1	323	1006.19	FF FF FF FF FF FF FF FF
5	65259	CI	Component Identification	250	Off Board Diagnostic-Servi...	63	5160.06	53 59 4E 45 52 2A 53 53 53 32 2D 30 35 2A 58 58 58 58 2A 55 4E 49 56 45 52 53 41 4C
6	65261	CCSS	Cruise Control/Vehicle Speed Setup	0	Engine #1	4	22417.30	69 64 30 FF FF FF FF FF
7	64892	DPFC1	DPF Control 1:E	0	Engine #1	324	1006.04	FF FF D0 34 FD FF FF FF
8	65214	EEC4	Electronic Engine Controller 4	0	Engine #1	4	50911.33	FF FF 00 00 FF FF FF FF
9	61440	ERC1	Electronic Retarder Controller 1	15	Retarder - Engine	3239	100.86	00 7D FF FF 0F FF FF FF
10	65263	EFL/P1	Engine Fluid Level/Pressure 1	0	Engine #1	647	503.86	FF FF FF FF FF FF FF FA
11	65243	EFL/P2	Engine Fluid Level/Pressure 2	0	Engine #1	647	503.86	FF FF FF FF FF FF FF FF
12	65253	HOURS	Engine Hours: Revolutions	0	Engine #1	2	50.24	1A EE 00 00 00 00 00 00
13	65262	ET1	Engine Temperature 1	0	Engine #1	323	1006.19	FF FF FF FF FF FF FF FF
14	65188	ET2	Engine Temperature 2	0	Engine #1	324	1006.08	FF FF FF FF FF FF FF FF
15	65213	FD1	Fan Drive #1	0	Engine #1	324	1006.02	FF FF FF FF FF FF FF FF
16	65257	LFC	Fuel Consumption (Liquid)	0	Engine #1	2	149.37	00 00 00 00 00 00 00 00
17	65266	LFE1	Fuel Economy (Liquid)	0	Engine #1	3239	100.86	00 00 00 00 00 00 FF FF
18	65217	VDHR	High Resolution Vehicle Distance	0	Engine #1	324	1006.17	FB 70 04 00 FB 70 04 00
19	65244	IO	Idle Operation	0	Engine #1	4	32437.36	00 00 00 00 00 00 00 00

- Decoding
- Counting
- Timing

J1939 Suspect Parameter Numbers

- Standards Interpretation



J1939 Status
Network Unavailable
Message Count: 0
Message Rate: 0 msg/sec
Client Disconnected 0 sec.

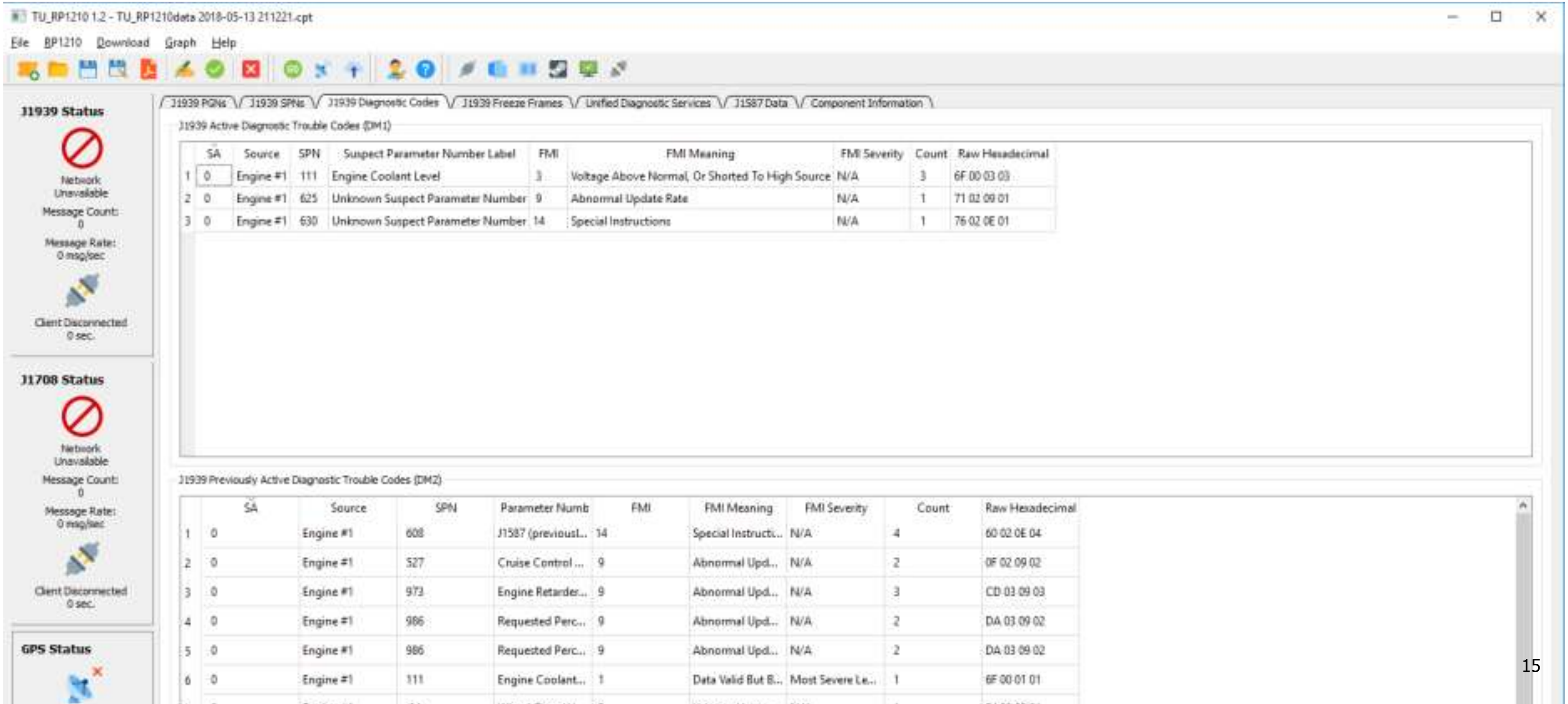
J1708 Status
Network Unavailable
Message Count: 0
Message Rate: 0 msg/sec
Client Disconnected 0 sec.

GPS Status
Disconnected

J1939 Suspect Parameter Numbers and Values

	Acronym	PGN	SA	Source	SPN	Suspect Parameter Number Label	Value	Units	Meaning
1	VI	65260	0	Engine #1	237	Vehicle Identification Number	1FUJGBDV1ALAR4676*	ASCII	
2	VI	65260	15	Retarder - Engine	237	Vehicle Identification Number	1FUJGBDV1ALAR4676*	ASCII	
3	VH	65255	0	Engine #1	246	Total Vehicle Hours	214748364.750	hours	Out of Range - High
4	VH	65255	0	Engine #1	248	Total Power Takeoff Hours	0.000	hours	
5	VEP1	65271	0	Engine #1	114	Net Battery Current	130	Amps	Out of Range - High
6	VEP1	65271	0	Engine #1	115	Alternator Current	255	Amps	Out of Range - High
7	VEP1	65271	0	Engine #1	158	Keyswitch Battery Potential	11.850	Volts	
8	VEP1	65271	0	Engine #1	167	Charging System Potential (Voltage)	3276.750	Volts	Out of Range - High
9	VEP1	65271	0	Engine #1	168	Battery Potential / Power Input 1	3276.750	Volts	Out of Range - High
10	VDHR	65217	0	Engine #1	917	High Resolution Total Vehicle Distance	1455335	meters	
11	VDHR	65217	0	Engine #1	918	High Resolution Trip Distance	1455335	meters	
12	VD	65248	0	Engine #1	244	Trip Distance	904.328	miles	
13	VD	65248	0	Engine #1	245	Total Vehicle Distance	904.328	miles	
14	TD	65254	0	Engine #1	1601	Local minute offset	-7245	minutes	Out of Range - Low
15	TD	65254	0	Engine #1	1602	Local hour offset	-449745	hours	Out of Range - Low
16	TD	65254	0	Engine #1	959	Seconds	3	Seconds	
17	TD	65254	0	Engine #1	960	Minutes	2	minutes	
18	TD	65254	0	Engine #1	961	Hours	2	hours	
19	TD	65254	0	Engine #1	962	Day	14	Days	
20	TD	65254	0	Engine #1	963	Month	5	Months	
21	TD	65254	0	Engine #1	964	Year	2018	Years	
22	TC	65245	0	Engine #1	103	Engine Turbocharger 1 Speed	262140	rpm	Out of Range - High
23	TC	65245	0	Engine #1	104	Engine Turbocharger Lube Oil Pressure 1	147.938	psi	Out of Range - High
24	TC	65245	0	Engine #1	1665	Engine Turbocharger Oil Level Switch	3	bit	Not available
25	SOFT	65242	0	Engine #1	234	Software Identification	004*003*000*000*R**a*018*000*08*11*10*12*00*0<.0053.00176*	ASCII	

J1939 Diagnostic Codes (DM1 and DM2)



J1939 Status
Network Unavailable
Message Count: 0
Message Rate: 0 msg/sec
Client Disconnected 0 sec.

J1708 Status
Network Unavailable
Message Count: 0
Message Rate: 0 msg/sec
Client Disconnected 0 sec.

GPS Status

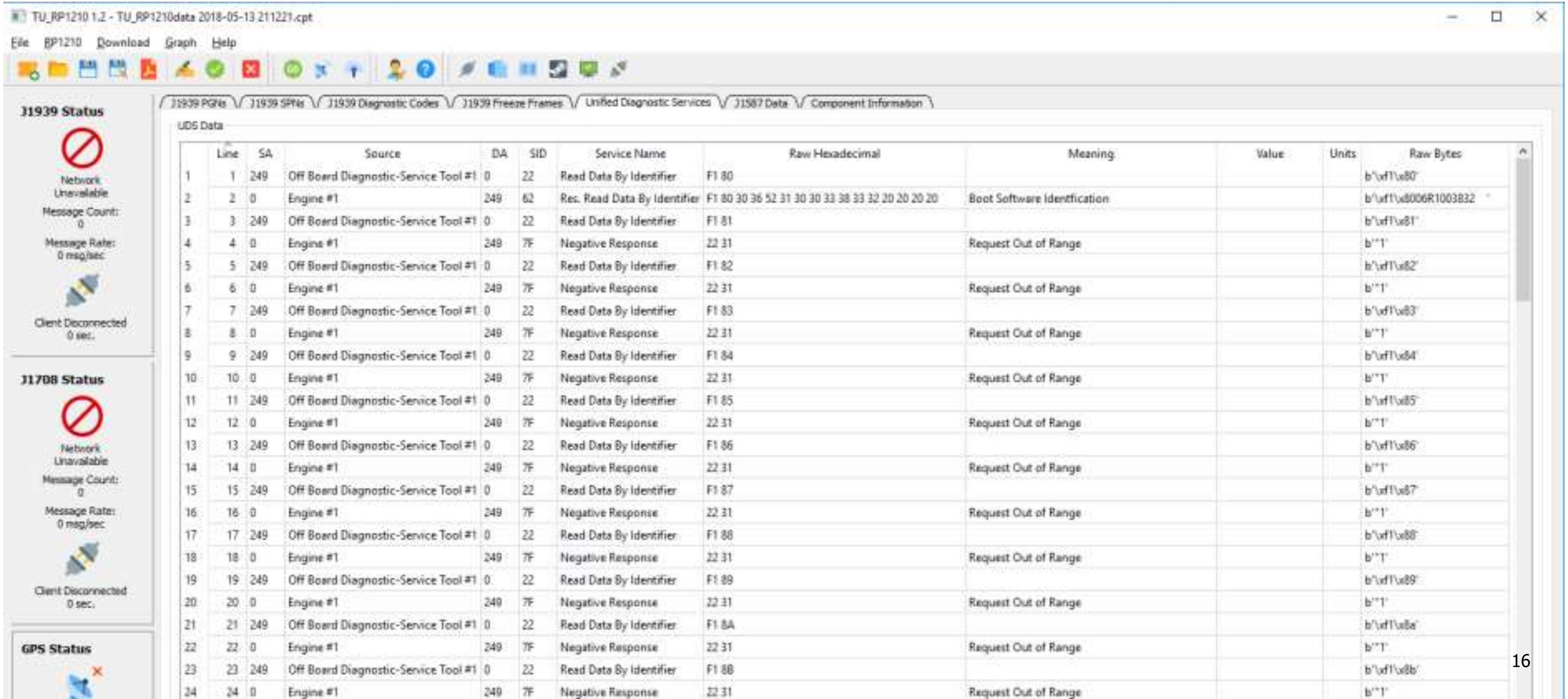
J1939 Active Diagnostic Trouble Codes (DM1)

	SA	Source	SPN	Suspect Parameter Number Label	FMI	FMI Meaning	FMI Severity	Count	Raw Hexadecimal
1	0	Engine #1	111	Engine Coolant Level	3	Voltage Above Normal, Or Shorted To High Source	N/A	3	6F 00 03 03
2	0	Engine #1	625	Unknown Suspect Parameter Number	9	Abnormal Update Rate	N/A	1	71 02 09 01
3	0	Engine #1	630	Unknown Suspect Parameter Number	14	Special Instructions	N/A	1	76 02 0E 01

J1939 Previously Active Diagnostic Trouble Codes (DM2)

	SA	Source	SPN	Parameter Numb	FMI	FMI Meaning	FMI Severity	Count	Raw Hexadecimal
1	0	Engine #1	608	J1587 (previousl...	14	Special Instructi...	N/A	4	60 02 0E 04
2	0	Engine #1	527	Cruise Control ...	9	Abnormal Upd...	N/A	2	0F 02 09 02
3	0	Engine #1	973	Engine Retarder...	9	Abnormal Upd...	N/A	3	CD 03 09 03
4	0	Engine #1	986	Requested Perc...	9	Abnormal Upd...	N/A	2	DA 03 09 02
5	0	Engine #1	986	Requested Perc...	9	Abnormal Upd...	N/A	2	DA 03 09 02
6	0	Engine #1	111	Engine Coolant...	1	Data Valid But B...	Most Severe Le...	1	6F 00 01 01

ISO-14229:
Unified Diagnostic Services (UDS)



TU_RP1210 1.2 - TU_RP1210data 2018-05-13 211221.cpt

J1939 Status

Network Unavailable

Message Count: 0

Message Rate: 0 msg/sec

Client Disconnected 0 sec.

J1708 Status

Network Unavailable

Message Count: 0

Message Rate: 0 msg/sec

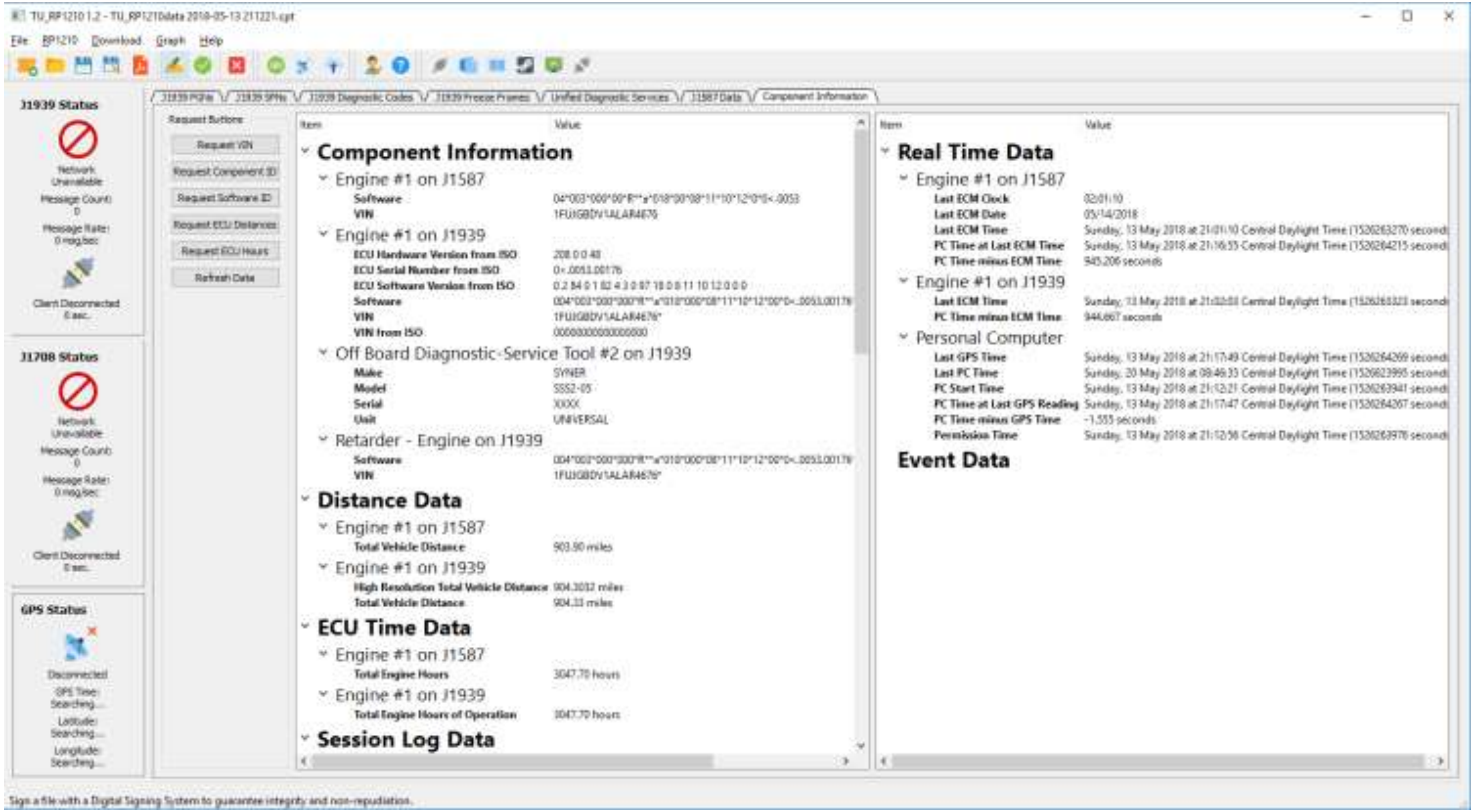
Client Disconnected 0 sec.

GPS Status

UDS Data

	Line	SA	Source	DA	SID	Service Name	Raw Hexadecimal	Meaning	Value	Units	Raw Bytes
1	1	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 80				b'\xf1\x80'
2	2	0	Engine #1	249	62	Res. Read Data By Identifier	F1 80 30 36 52 31 30 30 33 38 33 32 20 20 20 20	Boot Software Identfication			b'\xf1\x8006R1003832
3	3	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 81				b'\xf1\x81'
4	4	0	Engine #1	249	7F	Negative Response	22 31	Request Out of Range			b'"1'
5	5	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 82				b'\xf1\x82'
6	6	0	Engine #1	249	7F	Negative Response	22 31	Request Out of Range			b'"1'
7	7	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 83				b'\xf1\x83'
8	8	0	Engine #1	249	7F	Negative Response	22 31	Request Out of Range			b'"1'
9	9	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 84				b'\xf1\x84'
10	10	0	Engine #1	249	7F	Negative Response	22 31	Request Out of Range			b'"1'
11	11	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 85				b'\xf1\x85'
12	12	0	Engine #1	249	7F	Negative Response	22 31	Request Out of Range			b'"1'
13	13	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 86				b'\xf1\x86'
14	14	0	Engine #1	249	7F	Negative Response	22 31	Request Out of Range			b'"1'
15	15	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 87				b'\xf1\x87'
16	16	0	Engine #1	249	7F	Negative Response	22 31	Request Out of Range			b'"1'
17	17	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 88				b'\xf1\x88'
18	18	0	Engine #1	249	7F	Negative Response	22 31	Request Out of Range			b'"1'
19	19	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 89				b'\xf1\x89'
20	20	0	Engine #1	249	7F	Negative Response	22 31	Request Out of Range			b'"1'
21	21	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 8A				b'\xf1\x8a'
22	22	0	Engine #1	249	7F	Negative Response	22 31	Request Out of Range			b'"1'
23	23	249	Off Board Diagnostic-Service Tool #1	0	22	Read Data By Identifier	F1 8B				b'\xf1\x8b'
24	24	0	Engine #1	249	7F	Negative Response	22 31	Request Out of Range			b'"1'

Component Information Summary



J1939 Status
Network Unavailable
Message Count: 0
Message Rate: 0 msg/sec
Client Disconnected 0 sec.

J1708 Status
Network Unavailable
Message Count: 0
Message Rate: 0 msg/sec
Client Disconnected 0 sec.

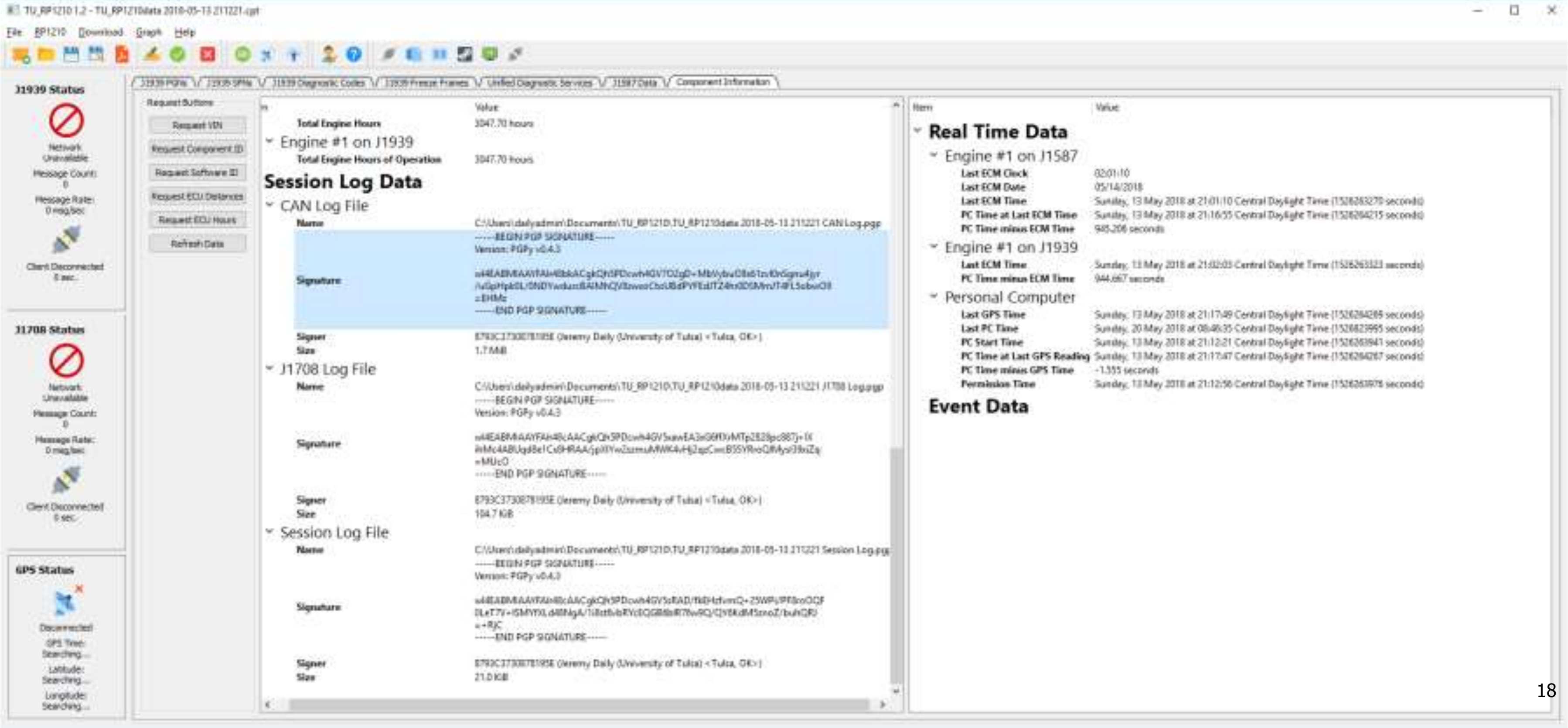
GPS Status
Disconnected
GPS Time: Searching...
Latitude: Searching...
Longitude: Searching...

```
Item                                        Value
Component Information
  Engine #1 on J1587
      Software                              04*003*000*00*R**a*018*00*08*11*10*12*0*0<.0053
      VIN                                   1FUJGBDV1ALAR4676
  Engine #1 on J1939
      ECU Hardware Version from ISO         208 0 0 48
      ECU Serial Number from ISO            0<.0053.00176
      ECU Software Version from ISO         0 2 84 0 1 82 4 3 0 87 18 0 8 11 10 12 0 0 0
      Software                              004*003*000*000*R**a*010*000*08*11*10*12*00*0<.0053.00176
      VIN                                   1FUJGBDV1ALAR4676*
      VIN from ISO                          00000000000000000
  Off Board Diagnostic-Service Tool #2 on J1939
      Make                                  SYNER
      Model                                 SSS2-05
      Serial                                XXXX
      Unit                                  UNIVERSAL
  Retarder - Engine on J1939
      Software                              004*003*000*000*R**a*010*000*08*11*10*12*00*0<.0053.00176
      VIN                                   1FUJGBDV1ALAR4676*
Distance Data
  Engine #1 on J1587
      Total Vehicle Distance                903.90 miles
  Engine #1 on J1939
      High Resolution Total Vehicle Distance 904.3032 miles
      Total Vehicle Distance                904.33 miles
ECU Time Data
  Engine #1 on J1587
      Total Engine Hours                    3047.70 hours
  Engine #1 on J1939
      Total Engine Hours of Operation       3047.70 hours
Session Log Data
```

```
Item                          Value
Real Time Data
  Engine #1 on J1587
      Last ECM Clock              02:01:10
      Last ECM Date               05/14/2018
      Last ECM Time               Sunday, 13 May 2018 at 21:01:10 Central Daylight Time (1526263270 second
      PC Time at Last ECM Time    Sunday, 13 May 2018 at 21:16:55 Central Daylight Time (1526264215 second
      PC Time minus ECM Time      945.206 seconds
  Engine #1 on J1939
      Last ECM Time               Sunday, 13 May 2018 at 21:02:03 Central Daylight Time (1526263323 second
      PC Time minus ECM Time      944.667 seconds
  Personal Computer
      Last GPS Time               Sunday, 13 May 2018 at 21:17:49 Central Daylight Time (1526264269 second
      Last PC Time                Sunday, 20 May 2018 at 08:46:33 Central Daylight Time (1526823995 second
      PC Start Time               Sunday, 13 May 2018 at 21:12:21 Central Daylight Time (1526263941 second
      PC Time at Last GPS Reading Sunday, 13 May 2018 at 21:17:47 Central Daylight Time (1526264267 second
      PC Time minus GPS Time      -1.555 seconds
      Permission Time             Sunday, 13 May 2018 at 21:12:56 Central Daylight Time (1526263976 second
Event Data
```

Sign a file with a Digital Signing System to guarantee integrity and non-repudiation.

PGP and Cryptography Implementations



```
J1939 Status
Network Unavailable
Message Count: 0
Message Rate: 0 msg/sec
Client Disconnected 0 sec.

J1708 Status
Network Unavailable
Message Count: 0
Message Rate: 0 msg/sec
Client Disconnected 0 sec.

GPS Status
Disconnected
GPS Time: Searching...
Latitude: Searching...
Longitude: Searching...
```

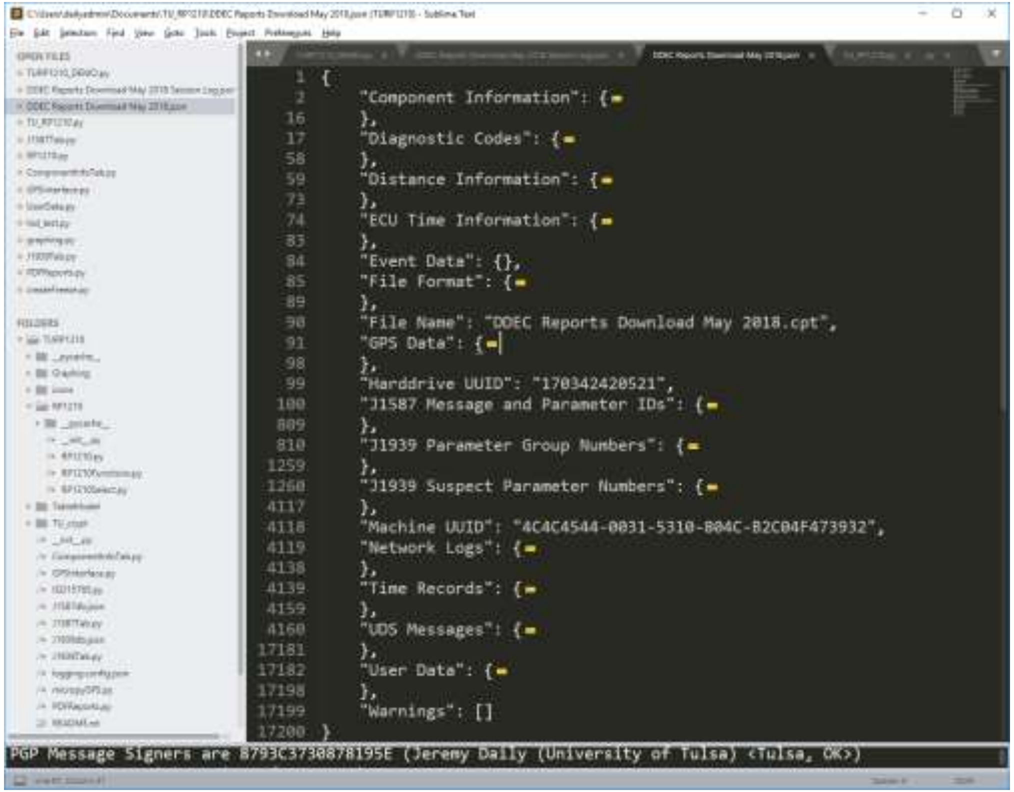
```
                                     Value
      Total Engine Hours             3047.70 hours
  Engine #1 on J1939
      Total Engine Hours of Operation 3047.70 hours
Session Log Data
  CAN Log File
      Name        C:\Users\dailyadmin\Documents\TU_RP1210\TU_RP1210data 2018-05-13 211221 CAN Log.pgp
                  -----BEGIN PGP SIGNATURE-----
                  Version: PGPy v0.4.3

      Signature   wl4EABMIAAYFAlr4lBbkACgkQh5PDcwh4GV7O2gD+MbVybuO8x61zu0nSgnu4jyr
                  /uGpHpk0L/0NDYwdunBAlMhQVBzwezCbdUBdPYFEdJTZ4nx0DSMmJT4FL5obvO8
                  =EHMz
                  -----END PGP SIGNATURE-----
      Signer      8793C3730878195E (Jeremy Daily (University of Tulsa) <Tulsa, OK>)
      Size        1.7 MiB
  J1708 Log File
      Name        C:\Users\dailyadmin\Documents\TU_RP1210\TU_RP1210data 2018-05-13 211221 J1708 Log.pgp
                  -----BEGIN PGP SIGNATURE-----
                  Version: PGPy v0.4.3

      Signature   wl4EABMIAAYFAlr4BcAACgkQh5PDcwh4GV5xawEA3xG6fIXvMTp2828pc887j+IX
                  iWMc4ABUqd8e1Cs8HRAA/jpXIYwZszmuMWK4vHj2qzCwcB5SYRroQlMysI3liZq
                  =MUcO
                  -----END PGP SIGNATURE-----

      Signer      8793C3730878195E (Jeremy Daily (University of Tulsa) <Tulsa, OK>)
      Size        104.7 KiB
  Session Log File
      Name        C:\Users\dailyadmin\Documents\TU_RP1210\TU_RP1210data 2018-05-13 211221 Session Log.pgp
                  -----BEGIN PGP SIGNATURE-----
                  Version: PGPy v0.4.3

      Signature   wl4EABMIAAYFAlr4BcAACgkQh5PDcwh4GV5sRAD/9dHzfvmQ+25WPi/PF8ooOQF
                  0LeT7V+ISMYfXLd48NgA/1i8stfvbRYcbQGB6bR76wRQ/QY6KdM5znoZ/buhQRJ
                  =+RJC
                  -----END PGP SIGNATURE-----

      Signer      8793C3730878195E (Jeremy Daily (University of Tulsa) <Tulsa, OK>)
      Size        21.0 KiB
```

```
Item                              Value
Real Time Data
  Engine #1 on J1587
      Last ECM Clock              02:01:10
      Last ECM Date               05/14/2018
      Last ECM Time               Sunday, 13 May 2018 at 21:01:10 Central Daylight Time (1526263270 seconds)
      PC Time at Last ECM Time    Sunday, 13 May 2018 at 21:16:55 Central Daylight Time (1526264215 seconds)
      PC Time minus ECM Time      945.206 seconds
  Engine #1 on J1939
      Last ECM Time               Sunday, 13 May 2018 at 21:02:03 Central Daylight Time (1526263323 seconds)
      PC Time minus ECM Time      944.667 seconds
  Personal Computer
      Last GPS Time               Sunday, 13 May 2018 at 21:17:49 Central Daylight Time (1526264269 seconds)
      Last PC Time                Sunday, 20 May 2018 at 08:46:35 Central Daylight Time (1526823995 seconds)
      PC Start Time               Sunday, 13 May 2018 at 21:12:21 Central Daylight Time (1526263941 seconds)
      PC Time at Last GPS Reading Sunday, 13 May 2018 at 21:17:47 Central Daylight Time (1526264267 seconds)
      PC Time minus GPS Time      -1.355 seconds
      Permission Time             Sunday, 13 May 2018 at 21:12:56 Central Daylight Time (1526263976 seconds)
Event Data
```

Open Source Framework

- Available on PyPi
- Uses PyQT5
- REST for Web Applications

- Teaching Tool
- RP1210 Function Validation
- Data Analysis

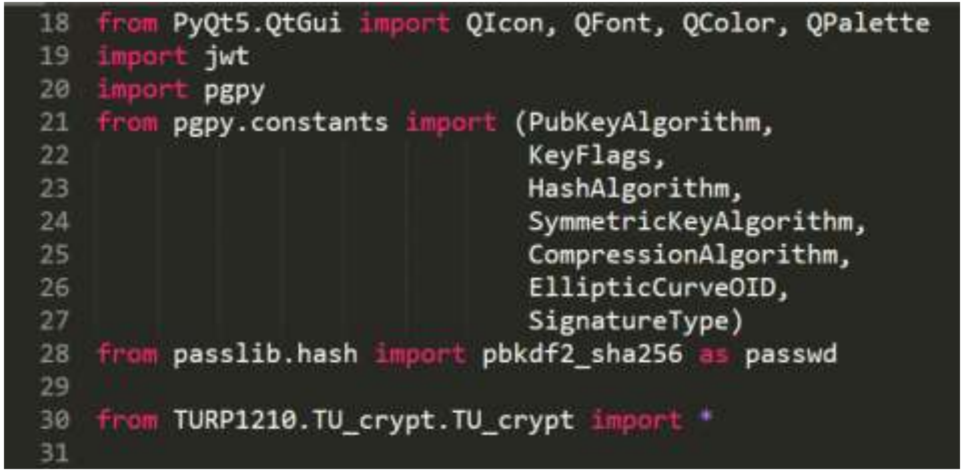

Sublime Text
File Edit Selection Find View Goto Tools Project Preferences Help
OPEN FILES
TU_RP1210.py
FOLDERS
RP1210
DDEC Reports Download May 2018.json

```
{
    "Component Information": {…
    },
    "Diagnostic Codes": {…
    },
    "Distance Information": {…
    },
    "ECU Time Information": {…
    },
    "Event Data": {},
    "File Format": {…
    },
    "File Name": "DDEC Reports Download May 2018.cpt",
    "GPS Data": {…
    },
    "Harddrive UUID": "170342420521",
    "J1587 Message and Parameter IDs": {…
    },
    "J1939 Parameter Group Numbers": {…
    },
    "J1939 Suspect Parameter Numbers": {…
    },
    "Machine UUID": "4C4C4544-0031-5310-804C-B2C04F473932",
    "Network Logs": {…
    },
    "Time Records": {…
    },
    "UDS Messages": {…
    },
    "User Data": {…
    },
    "Warnings": []
}
```

```
PGP Message Signers are 8793C3730878195E (Jeremy Daily (University of Tulsa) <Tulsa, OK>)
```

Data Storage

- JSON file for decoded data
- CSV log files for Vehicle Networks
- PDF Report generator using Reportlab
- Pretty Good Privacy (PGP) implementation for file signing



```
from PyQt5.QtGui import QIcon, QFont, QColor, QPalette
import jwt
import pgpy
from pgpy.constants import (PubKeyAlgorithm,
                            KeyFlags,
                            HashAlgorithm,
                            SymmetricKeyAlgorithm,
                            CompressionAlgorithm,
                            EllipticCurveOID,
                            SignatureType)
from passlib.hash import pbkdf2_sha256 as passwd

from TURP1210.TU_crypt.TU_crypt import *

```

Forget about the network…

CAN WE OBTAIN MEMORY CONTENTS THOUGH JTAG PORTS?

A Journey Into Chip Forensics

Duy Van
Undergraduate in Mechanical Engineering
duy-van@utulsa.edu

THE UNIVERSITY of TULSA
Student CyberTruck Experience

About me

- Born in Ho Chi Minh, Vietnam
- Former competitive badminton player
- Second home: Wichita, KS
- Been in the U.S for 6 years
- Car enthusiast

Cyber Security Minor at UTULSA

Additional Courses

- Intro to Cyber Security
- Computer Forensics
- Computer Security
- Secure Electronic Commerce

This is on top of a Mechanical Engineering degree…

Relevant Projects

- Password cracking
- Acquire and analyze computer’s hard drive
- Writing AES encryption from scratch using C
- Attack a virtual website with XSS, SQL injection, directory traversal, etc. and fix the vulnerabilities by changing source codes.

Purposes and Procedures

- Explore data patterns between RP1210 traffic logs and raw memory
- Download Dataplate and Sudden Deceleration using Cummins PowerSpec
- Collect raw data from FLASH and EEPROM through JTAG
- Compare the data and decode raw binary

ECM Used

Cummins ECU CM870

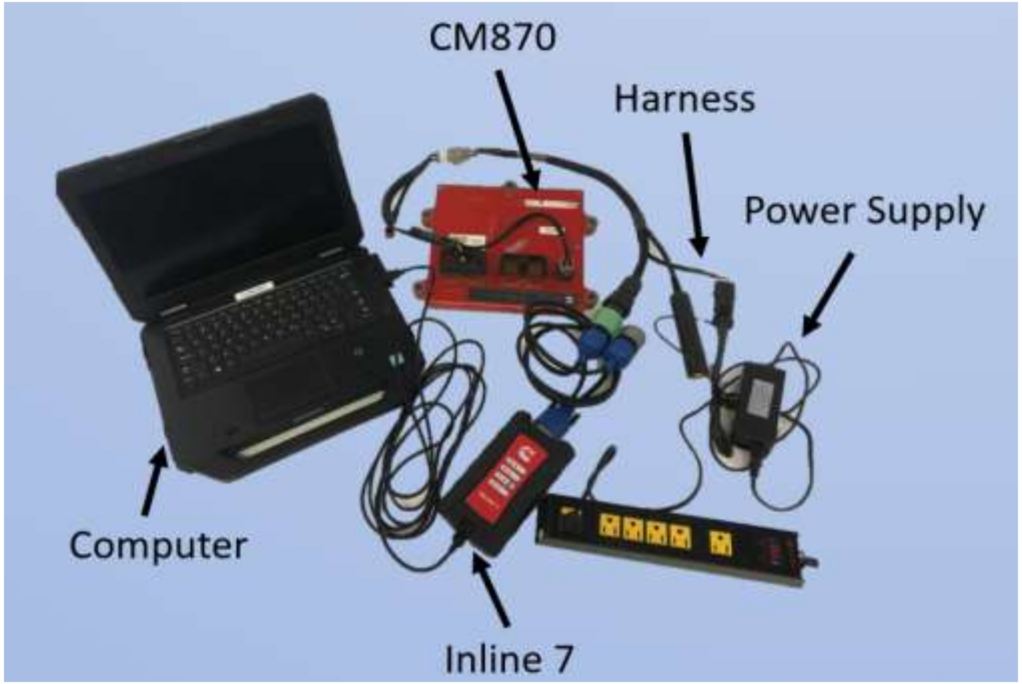
DOWNLOADING DATA FROM POWERSPEC

Tools

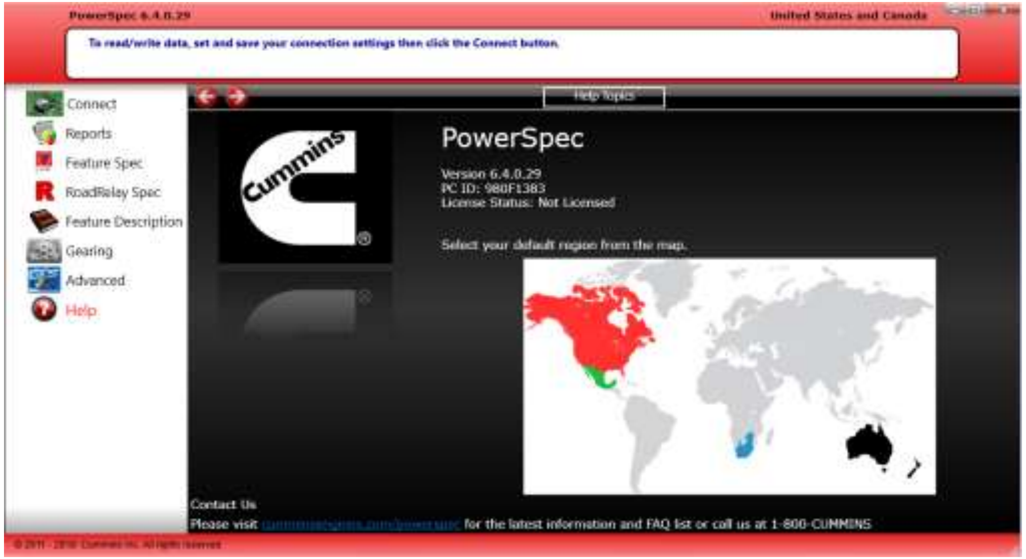
Inline 7
(Diagnostic Adapter)

Connecting
Harness

Setup



Software



PowerSpec 6.4.0.29

United States and Canada

To read/write data, set and save your connection settings then click the Connect button.

PowerSpec

Version 6.4.0.29
PC ID: 980F1383
License Status: Not Licensed

Select your default region from the map.

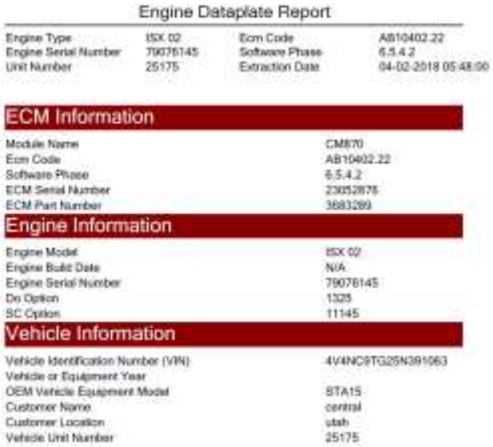
Contact Us

Please visit cumminsengines.com/powerspec for the latest information and FAQ list or call us at 1-800-CUMMINS

© 2011 - 2016 Cummins Inc. All rights reserved

Cummins PowerSpec

Downloading Data



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	23052878
ECM Part Number	3883289

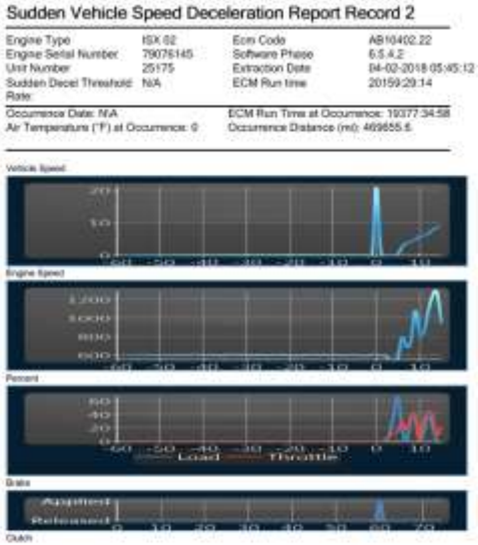
Engine Information

Engine Model	ISX 02
Engine Build Date	N/A
Engine Serial Number	79076145
Dn 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

Dataplate



Sudden Vehicle Speed Deceleration Report Record 2

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 05:45:12
Sudden Decel Threshold Rate:	N/A	ECM Run time	20159:29:14

Occurrence Date: N/A
Air Temperature (°F) at Occurrence: 0

ECM Run Time at Occurrence: 19377:34:58
Occurrence Distance (mi): 469655.6

Sudden Deceleration

COLLECTING RAW DATA FROM K-TAG

Tool

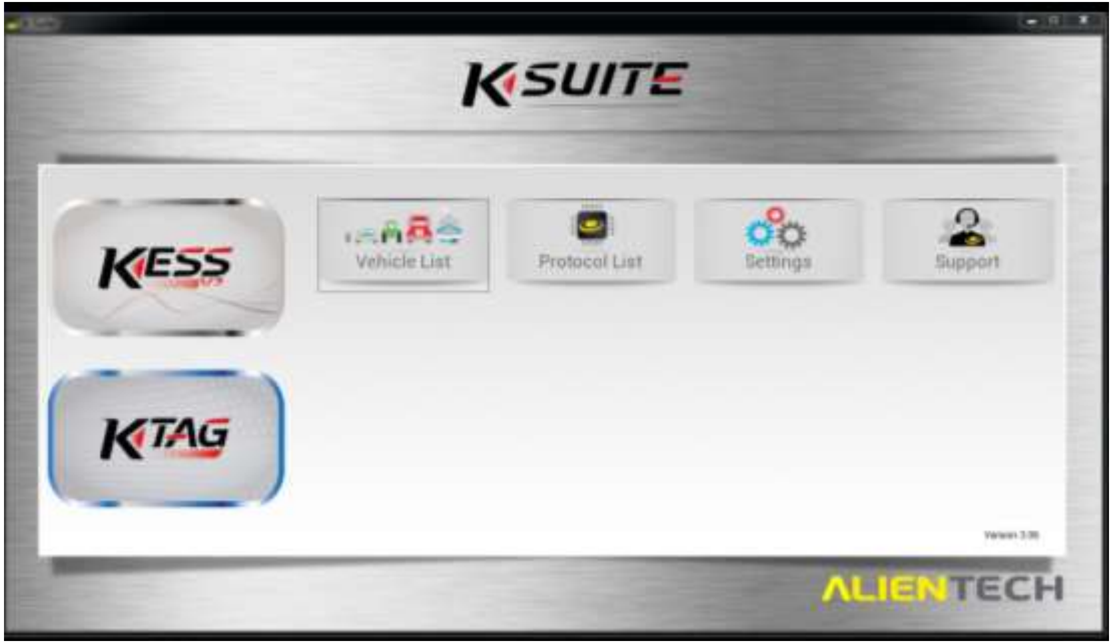
AlienTech KTAG Master Kit from a European Chip Tuning shop

Software Interaction

- Connect KTAG device to the computer

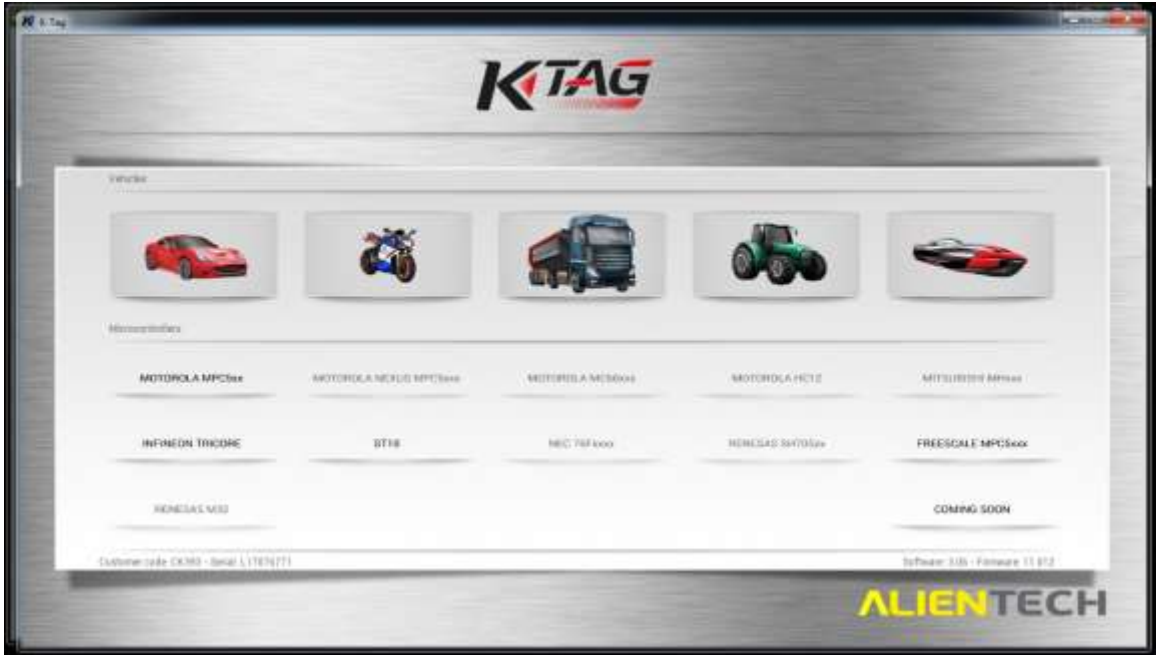
Software Interaction

- Run the K-Suite software from AlienTech



Software Interaction

- Select purchased version (KTAG in this case)

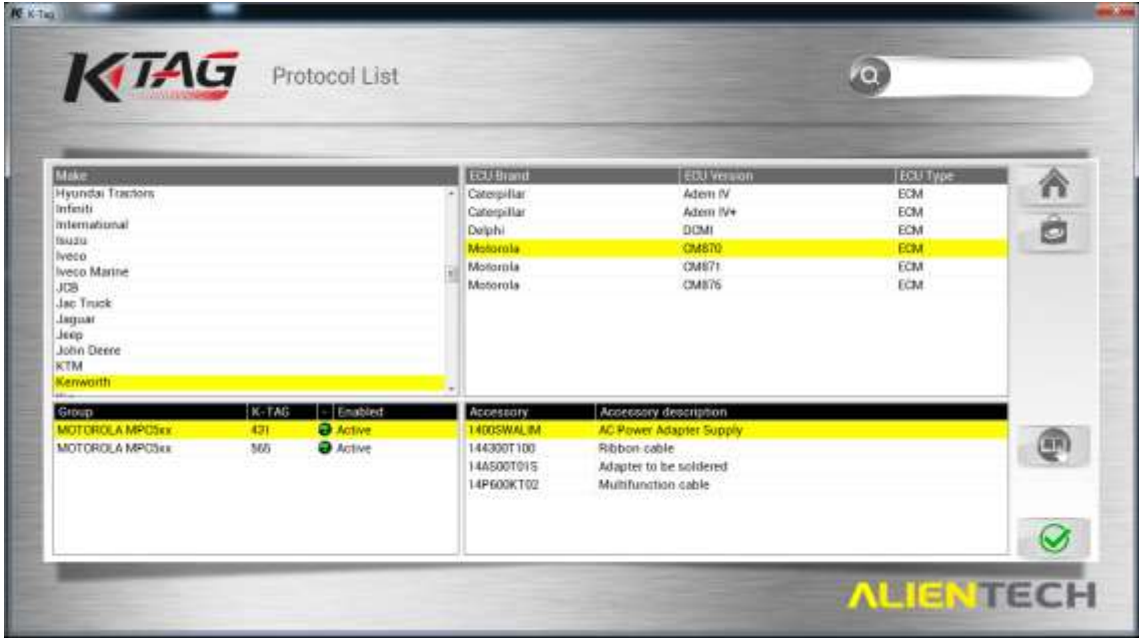


Software Interaction

- Purchased chip protocols will be in black font color and can be selected.
- Vehicle types can also be selected if chip protocol is unknown at this moment.

Software Interaction

- If chip protocol is known, choose the protocol



Make
Hyundai Tractors
Infiniti
International
Isuzu
Iveco
Iveco Marine
JCB
Jac Truck
Jaguar
Jeep
John Deere
KTM
Kenworth

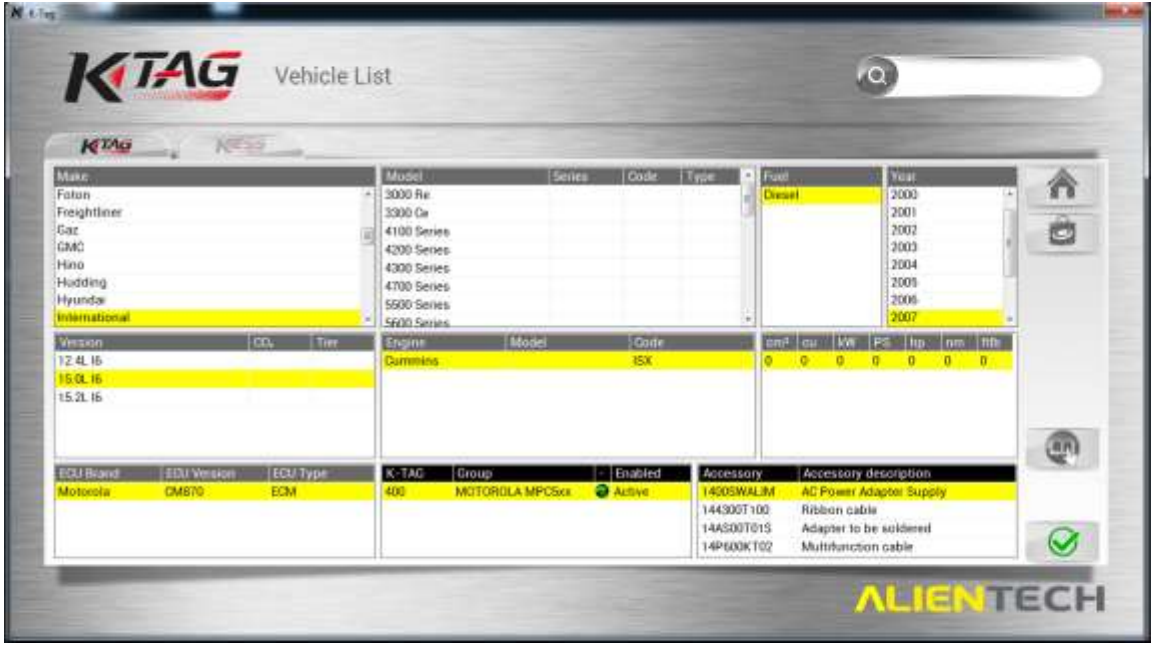
ECU Brand	ECU Version	ECU Type
Caterpillar	Adem IV	ECM
Caterpillar	Adem IV+	ECM
Delphi	DCMI	ECM
Motorola	CM870	ECM
Motorola	CM871	ECM
Motorola	CM876	ECM

Group	K-TAG	-	Enabled
MOTOROLA MPC5xx	431	●	Active
MOTOROLA MPC5xx	565	●	Active

Accessory	Accessory description
1400SWALIM	AC Power Adapter Supply
144300T100	Ribbon cable
14A500T015	Adapter to be soldered
14P600KT02	Multifunction cable

Software Interaction

- If vehicle type is known, choose the vehicle



Make
Foton
Freightliner
Gaz
GMC
Hino
Hudding
Hyundai
International

Model	Series	Code	Type
3000 Re			
3300 Ce			
4100 Series			
4200 Series			
4300 Series			
4700 Series			
5500 Series			
5600 Series			

Fuel
Diesel

Year
2000
2001
2002
2003
2004
2005
2006
2007

Version	CO_2	Tier
12.4L I6		
15.0L I6		
15.2L I6		

Engine	Model	Code
Cummins		ISX

cm³	cu	kW	PS	hp	nm	ftlb
0	0	0	0	0	0	0

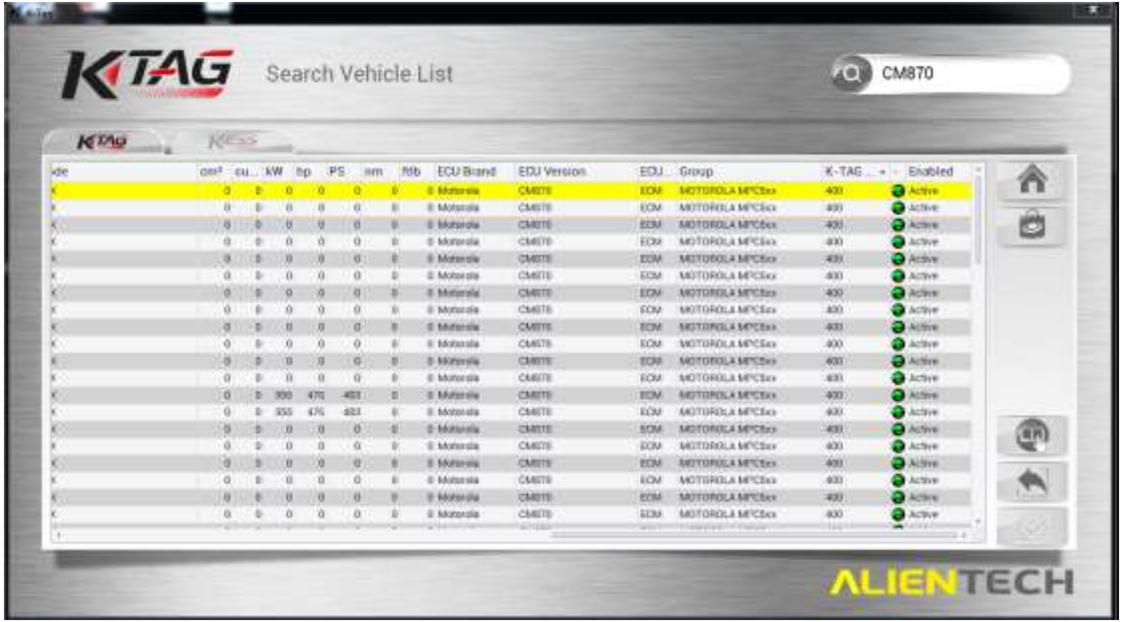
ECU Brand	ECU Version	ECU Type
Motorola	CM870	ECM

K-TAG	Group	-	Enabled
400	MOTOROLA MPC5xx	●	Active

Accessory	Accessory description
14OOSWALIM	AC Power Adapter Supply
144300T100	Ribbon cable
14AS00T01S	Adapter to be soldered
14P600KT02	Multifunction cable

Software Interaction

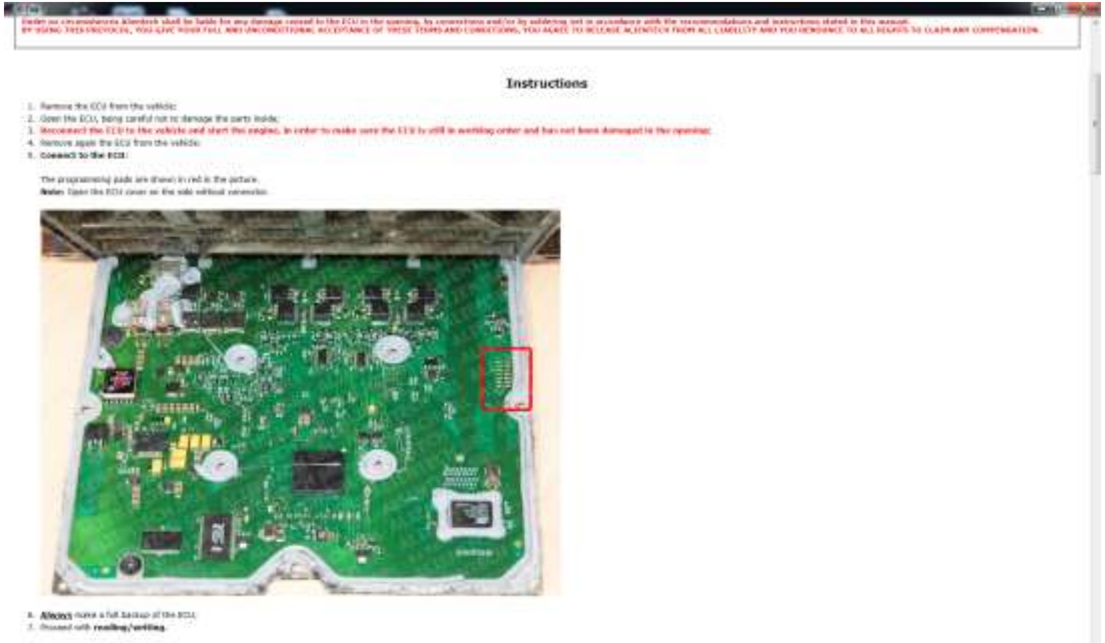
- Search option is also available



de	cm³	cu...	kW	hp	PS	nm	ftlb	ECU Brand	ECU Version	ECU	Group	K-TAG ...		Enabled
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	350	470	483	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	355	476	483	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active
K	0	0	0	0	0	0	0	Motorola	CM870	ECM	MOTOROLA MPC5xx	400	●	Active

Software Interaction

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



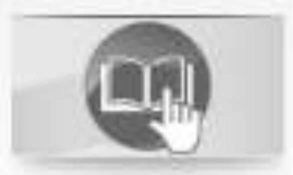
Under no circumstances Alientech shall be liable for any damage caused to the ECU in the opening, by connections and/or by soldering not in accordance with the recommendations and instructions stated in this manual.
BY USING THIS PROTOCOL, YOU GIVE YOUR FULL AND UNCONDITIONAL ACCEPTANCE OF THESE TERMS AND CONDITIONS. YOU AGREE TO RELEASE ALIENTECH FROM ALL LIABILITY AND YOU RENOUNCE TO ALL RIGHTS TO CLAIM ANY COMPENSATION.

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 the opening;
4. Remove again the ECU from the vehicle;
5. **Connect to the ECU**:

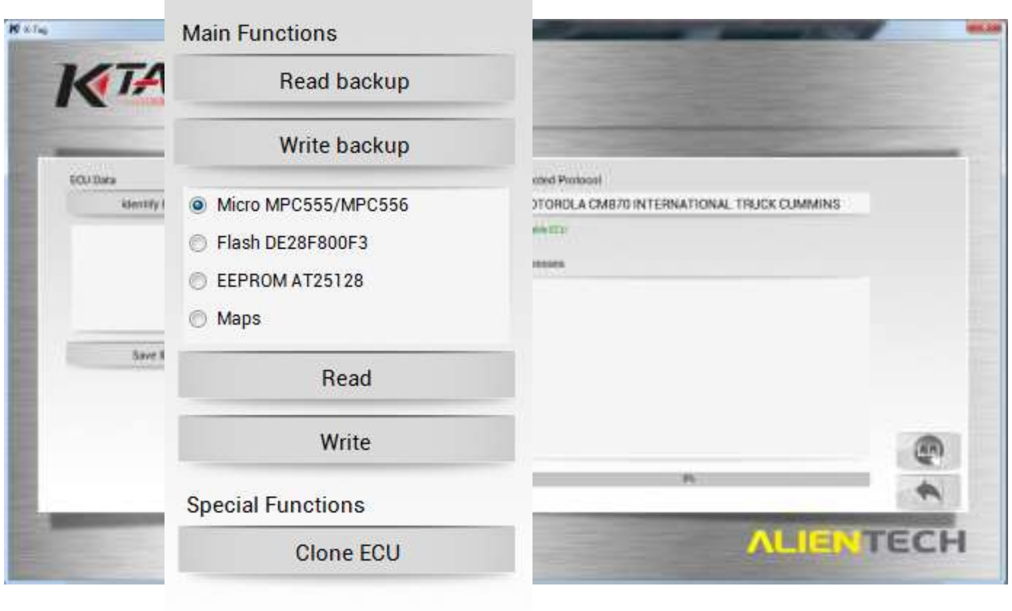
   The programming pads are shown in red in the picture.
   Note: Open the ECU cover on the side without connector.

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



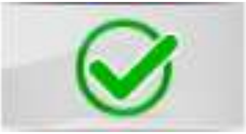
Software Interaction

- After following the instruction, click on the check icon for the main functions

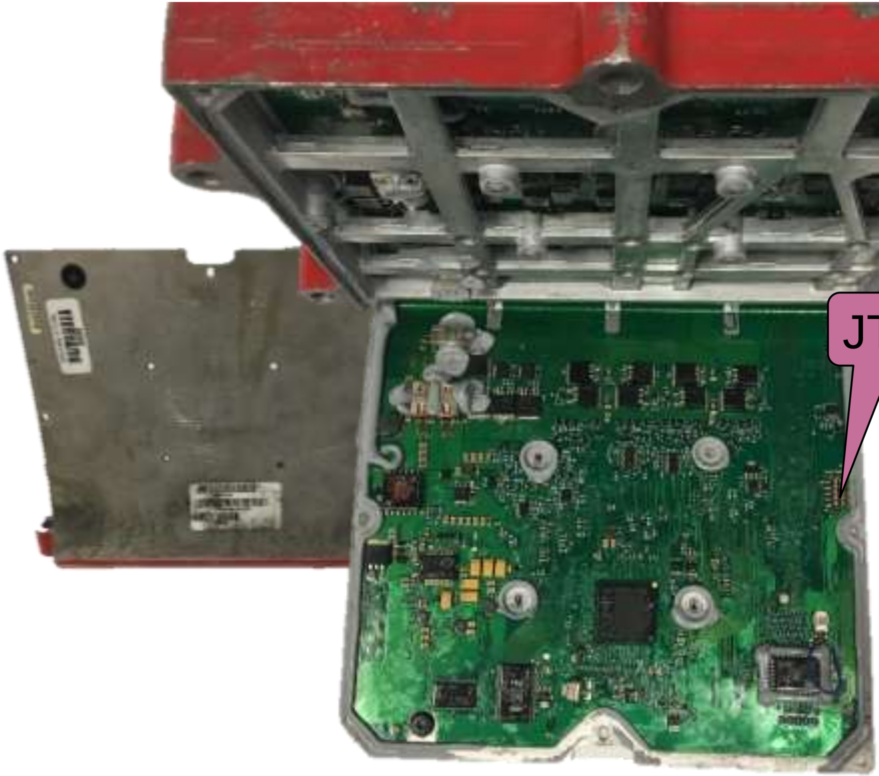


● Micro MPC555/MPC556
○ Flash DE28F800F3
○ EEPROM AT25128
○ Maps

...TOROLA CM870 INTERNATIONAL TRUCK CUMMINS



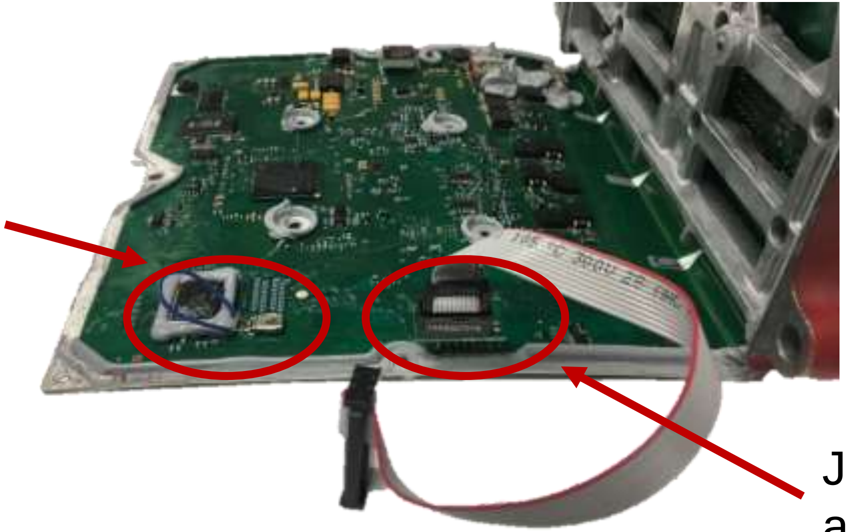
Hardware Demo



JTAG

Hardware Interaction

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

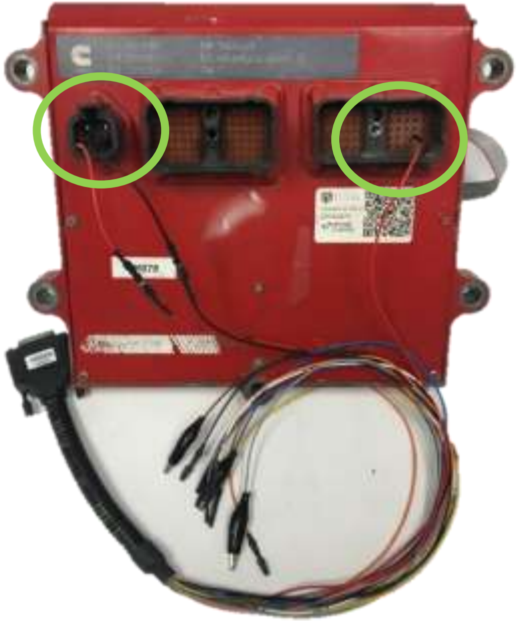


Bridge

JTAG pin headers and ribbon cable

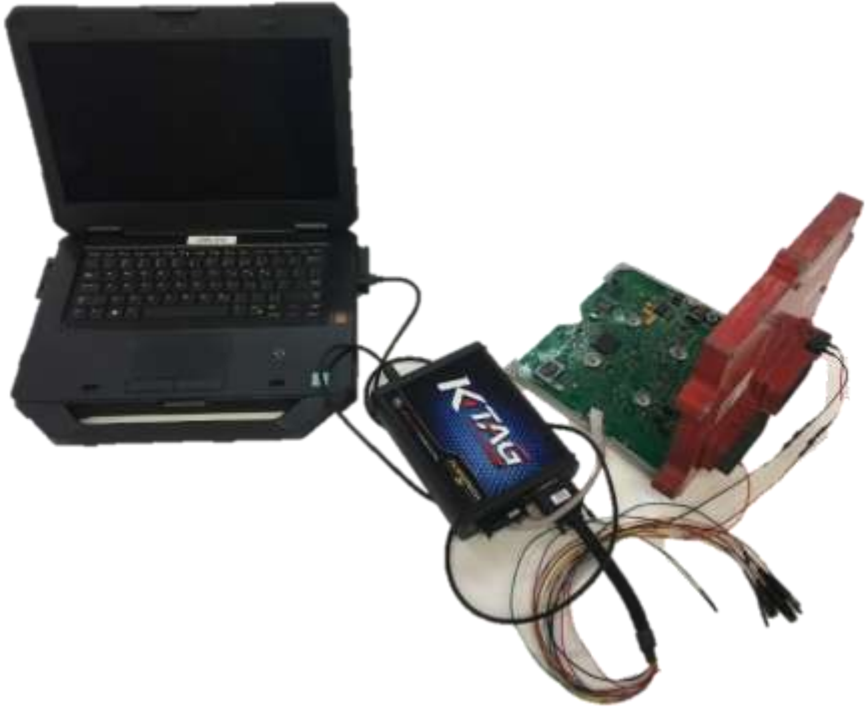
Hardware Interaction

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



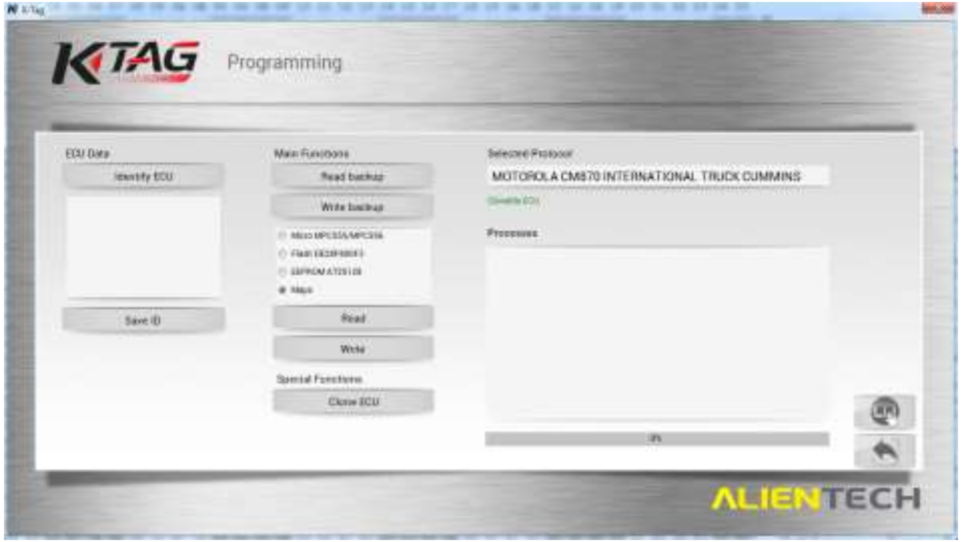
Setup

- Connect the KTAG to the ECU and the computer



Retrieving Data

- Select the desired function in the software
- In this case, select Maps and Read function

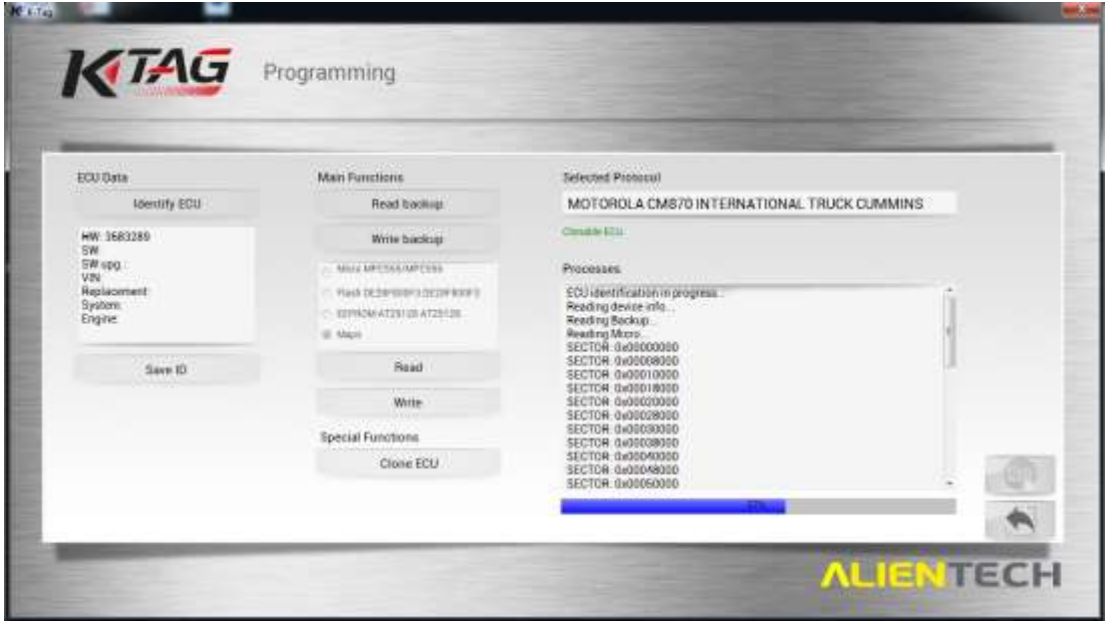


Selected Protocol: MOTOROLA CM870 INTERNATIONAL TRUCK CUMMINS

○ Micro MPC555/MPC556
○ Flash [illegible]
○ EEPROM [illegible]
● Maps

Retrieving Data

- Wait for the process to complete



HW: 3683289
SW:
SW upg.:
VIN:
Replacement:
System:
Engine:

Selected Protocol: MOTOROLA CM870 INTERNATIONAL TRUCK CUMMINS

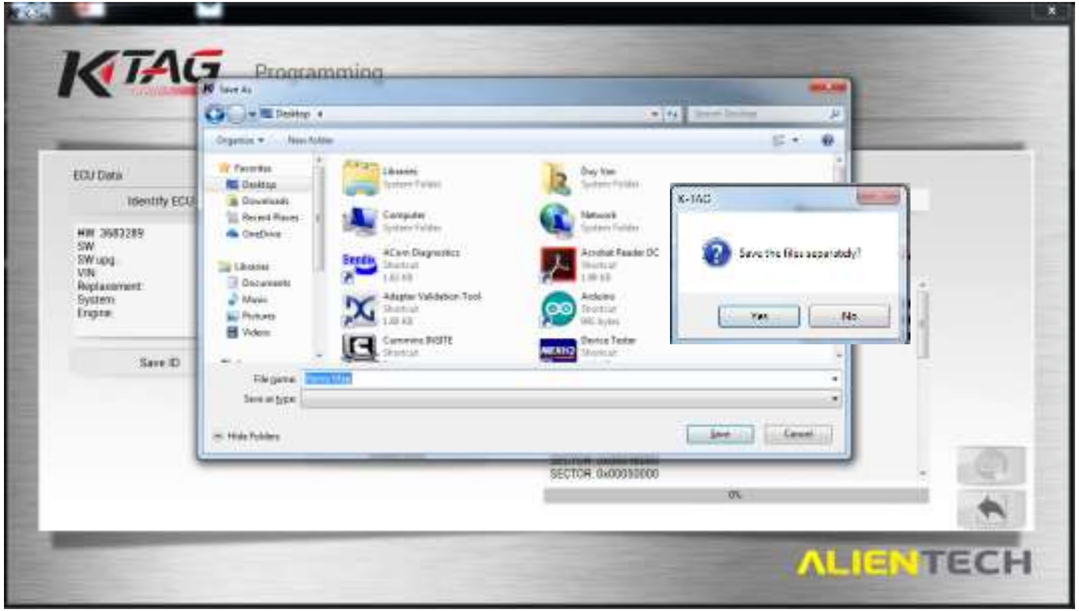
Clonable ECU

Processes

```
ECU identification in progress...
Reading device info...
Reading Backup...
Reading Micro...
SECTOR: 0x00000000
SECTOR: 0x00008000
SECTOR: 0x00010000
SECTOR: 0x00018000
SECTOR: 0x00020000
SECTOR: 0x00028000
SECTOR: 0x00030000
SECTOR: 0x00038000
SECTOR: 0x00040000
SECTOR: 0x00048000
SECTOR: 0x00050000
```

Retrieving Data

- Save the files separately



K-TAG

Save the files separately?

Yes No

ECU Data

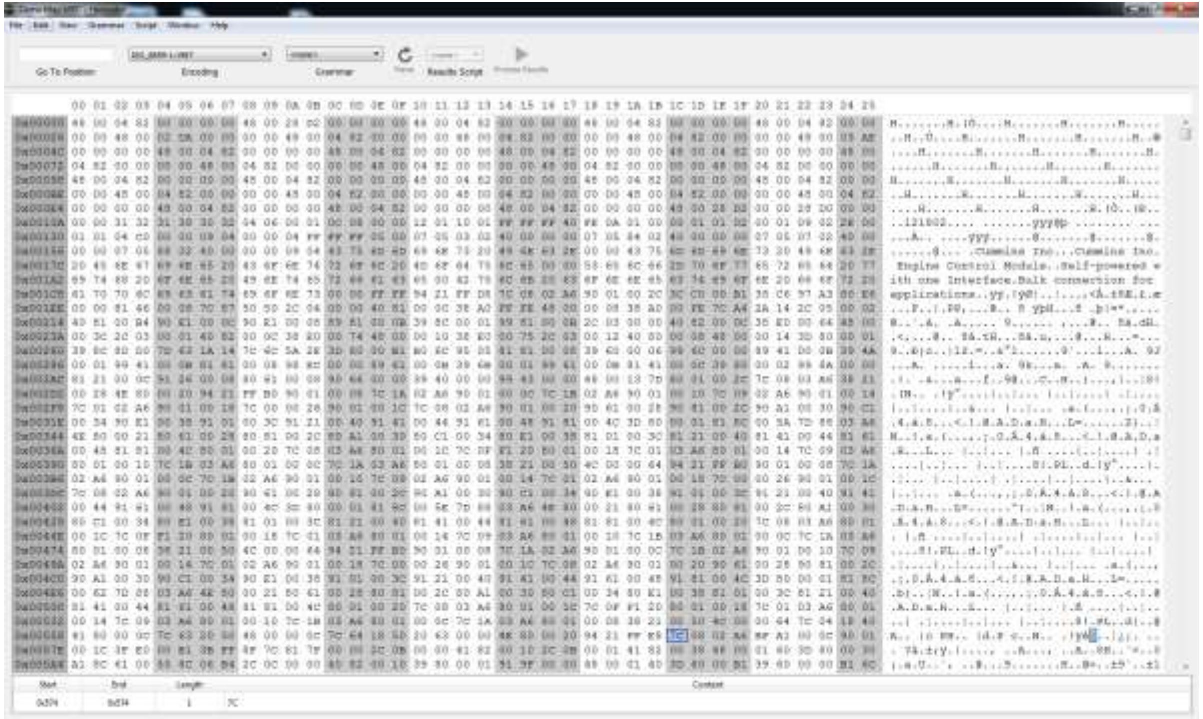
HW 3683289
SW
SW upg
VIN
Replacement:
System:
Engine:

SECTOR: 0x00030000

0%

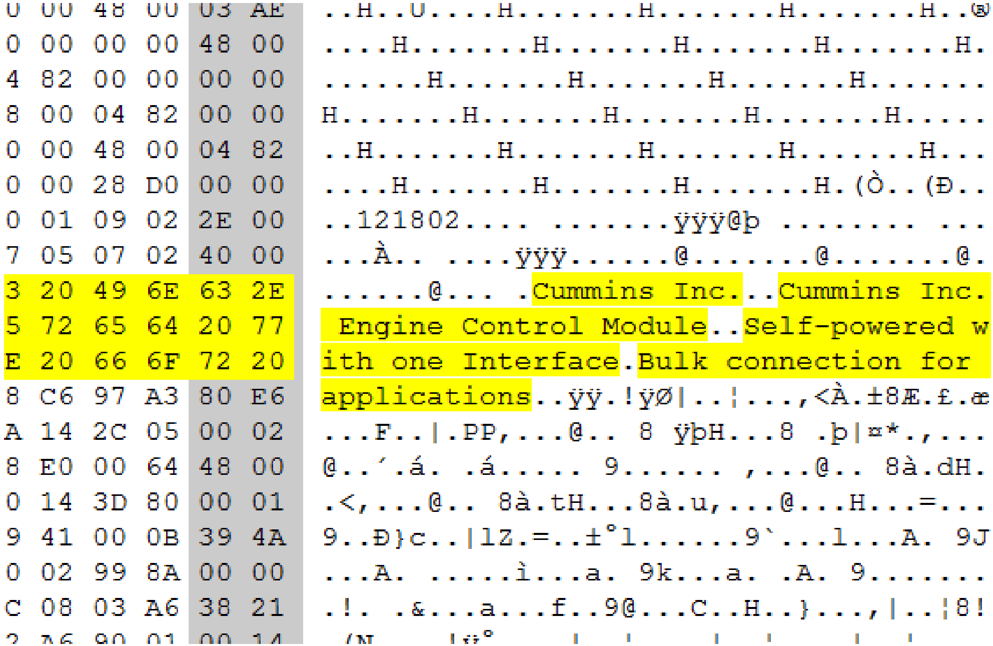
Data Analysis

- Use Hexinator to open the output MPC file



Data Analysis

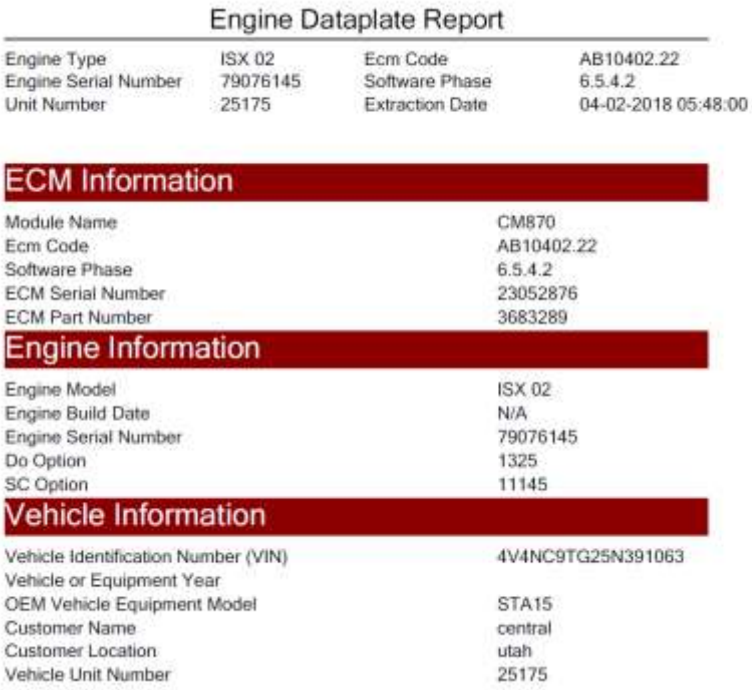
- Some meaningful strings are present indicating that the data is not encrypted



```
0 00 48 00 03 AE  ..H..U....H.......H.......H.......H..®
0 00 00 00 48 00  ....H.......H.......H.......H.......H.
4 82 00 00 00 00  ......H.......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 00  ....H.......H.......H.......H.(Ò..(Đ..
0 01 09 02 2E 00  ..121802.... .......ÿÿÿ@þ ........ ...
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 ÿþH...8 .þ|¤*.,...
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..Đ}c..|1Z.=..±°1......9`...1...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!
```

Data Analysis

- Closer look between PowerSpec vs EEPROM



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

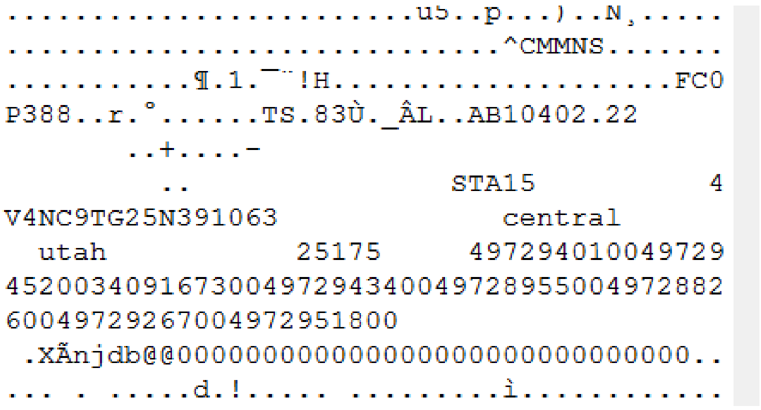
Module Name	CM870
Ecm Code	AB10402.22
Software Phase	6.5.4.2
ECM Serial Number	23052876
ECM Part Number	3683289

Engine Information

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

Vehicle Information

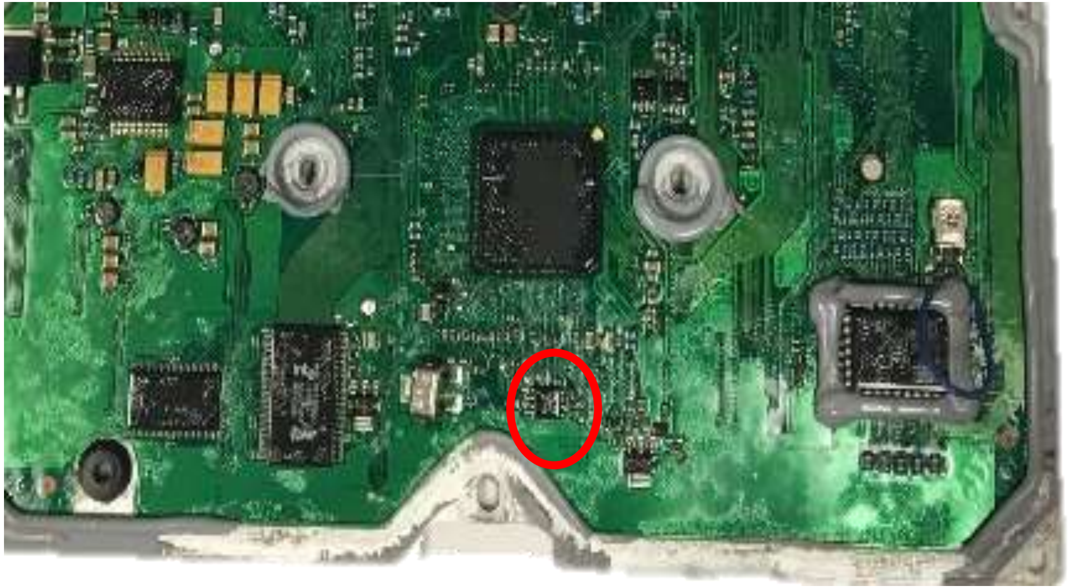
Vehicle Identification Number (VIN)	4V4NC9TG25N391063
Vehicle or Equipment Year	
OEM Vehicle Equipment Model	STA15
Customer Name	central
Customer Location	utah
Vehicle Unit Number	25175



```
........................u5..p...)..N,.....
.............................^CMMNS.......
...........¶.1.¯¨!H....................FC0
P388..r.°......TS.83Ù._ÂL..AB10402.22
       ..+....-
         ..               STA15          4
V4NC9TG25N391063             central
  utah           25175     497294010049729
452003409167300497294340049728955004972882
6004972926700497295180
 .XÃnjdb@@000000000000000000000000000000..
... . .....d.!..... .........ì............
```

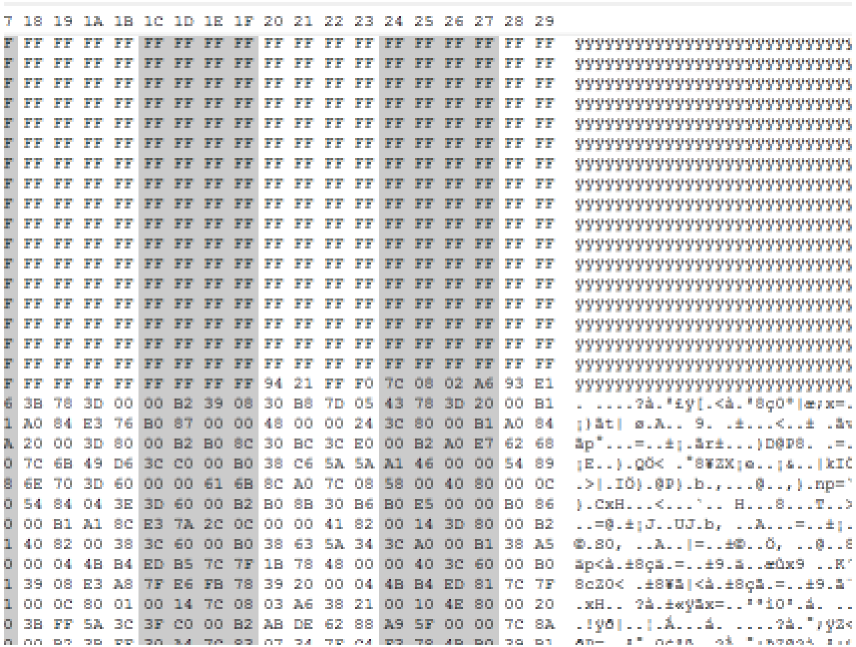
Data Analysis

- For CM870, EEPROM carries data plate information via ASCII



Data Analysis

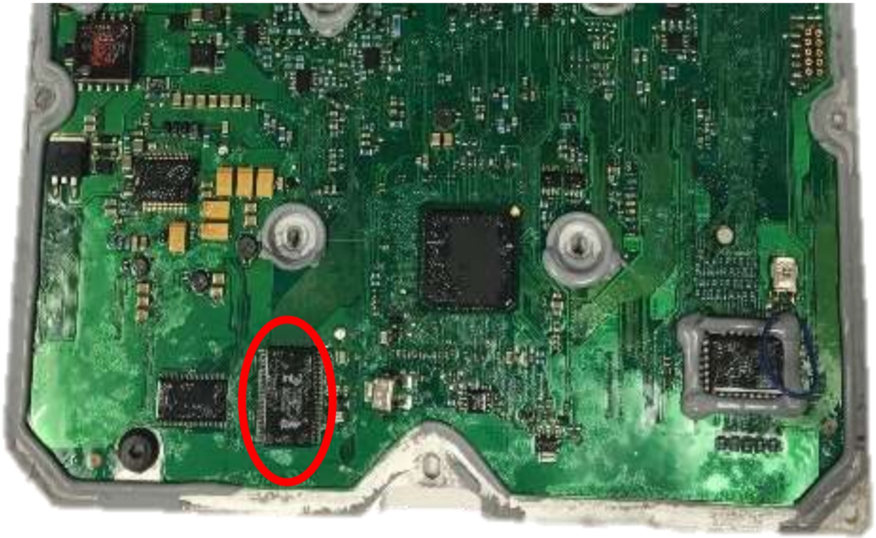
- Flash file from KTAG



```
7 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
F FF FF FF FF FF FF FF FF 94 21 FF F0 7C 08 02 A6 93 E1   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
6 3B 78 3D 00 00 B2 39 08 30 B8 7D 05 43 78 3D 20 00 B1   . ....?à.'£ÿ[.<à.'8çO'|æ;x=.
1 A0 84 E3 76 B0 87 00 00 48 00 00 24 3C 80 00 B1 A0 84   ¡}ãt| ø.A.. 9. .±...<..± .ã
A 20 00 3D 80 00 B2 B0 8C 30 BC 3C E0 00 B2 A0 E7 62 68   ãp"...=..±¦.ãr±...}D@P8. .=.
0 7C 6B 49 D6 3C C0 00 B0 38 C6 5A 5A A1 46 00 00 54 89   ¡E..}.QÖ< ."8¥ZX¡e..¦&..|kIÖ
8 6E 70 3D 60 00 00 61 6B 8C A0 7C 08 58 00 40 80 00 0C   .>|.IÖ}.@P}.b.,...@..,}.np='
0 54 84 04 3E 3D 60 00 B2 B0 8B 30 B6 B0 E5 00 00 B0 86   }.CxH...<...`.. H...8...T..>
0 00 B1 A1 8C E3 7A 2C 0C 00 00 41 82 00 14 3D 80 00 B2   ..=@.±¦J..UJ.b, ..A...=..±¦.
1 40 82 00 38 3C 60 00 B0 38 63 5A 34 3C A0 00 B1 38 A5   ©.80, ..A..|=..±©..Ô, ..@..8
0 00 04 4B B4 ED B5 7C 7F 1B 78 48 00 00 40 3C 60 00 B0   ãp<à.±8çã.=..±9.ã..æÛx9 ..K'
1 39 08 E3 A8 7F E6 FB 78 39 20 00 04 4B B4 ED 81 7C 7F   8cZO< .±8¥ã|<à.±8çã.=..±9.ã'
1 00 0C 80 01 00 14 7C 08 03 A6 38 21 00 10 4E 80 00 20   .xH.. ?à.±æÿãx=..''íO'.á. ..
0 3B FF 5A 3C 3F C0 00 B2 AB DE 62 88 A9 5F 00 00 7C 8A   .!ÿô|..¦.Á...á. ....?à.";ÿZ<
```

Data Analysis

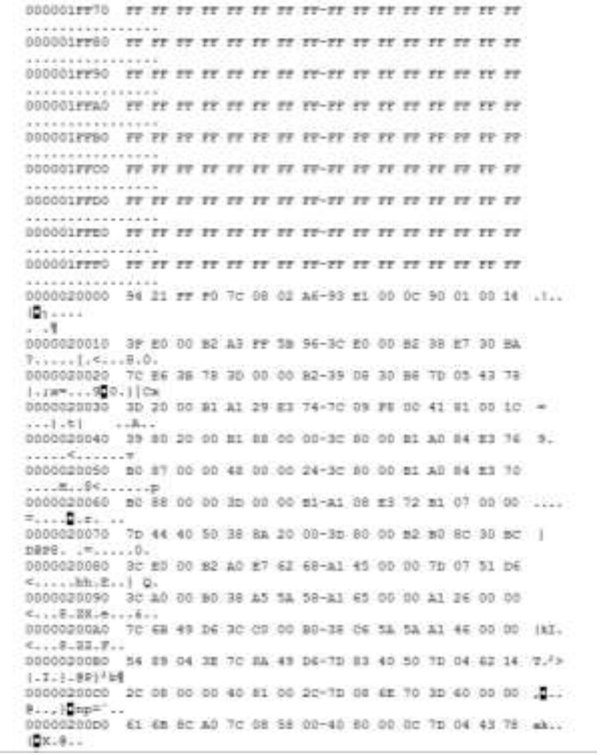
- Flash data can also be retrieved using individual chip reader



Xeltek Superpro 6000

Data Analysis

- Flash chip data should carry Sudden Decel Information (vehicle speed, engine RPM, etc.)
- Not easy to find the data location

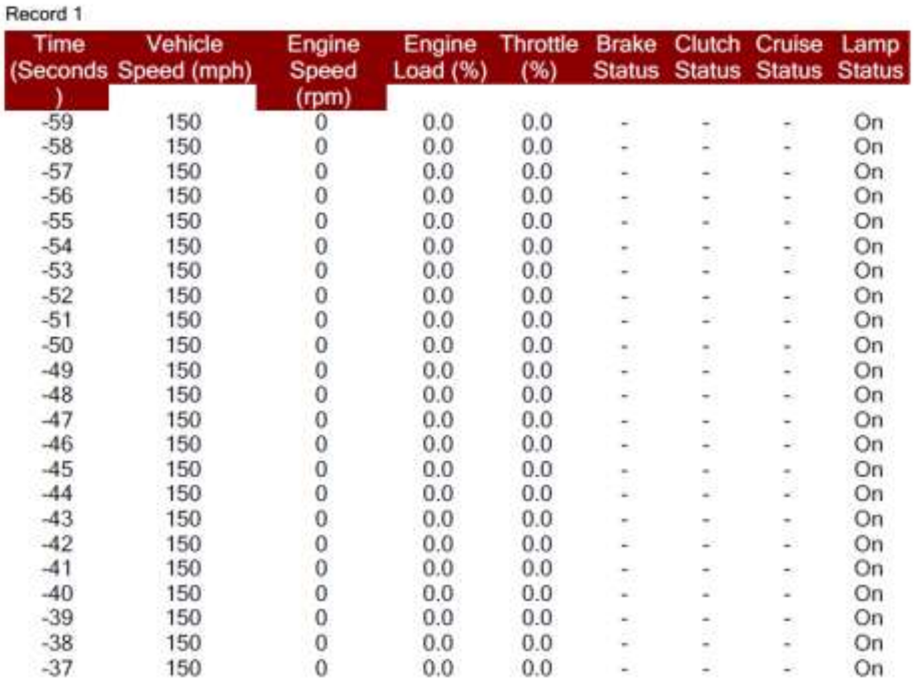


```
000001FF70  FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF
................
000001FF80  FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF
................
000001FF90  FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF
................
000001FFA0  FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF
................
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 3B 96-3C E0 00 B2 38 E7 30 BA
?.....|.<...8.0.
0000020020  7C E6 3B 78 3D 00 00 B2-39 08 30 B6 7D 05 43 78
|.;x=...9■0.}|Cx
0000020030  3D 20 00 B1 A1 29 E3 74-7C 09 FE 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.²>
|.I.}.@P}²b¶
00000200C0  2C 08 00 00 40 81 00 2C-7D 08 6E 70 3D 40 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:

- Vehicle speed for Record 1 has 150 mph for the first 60s

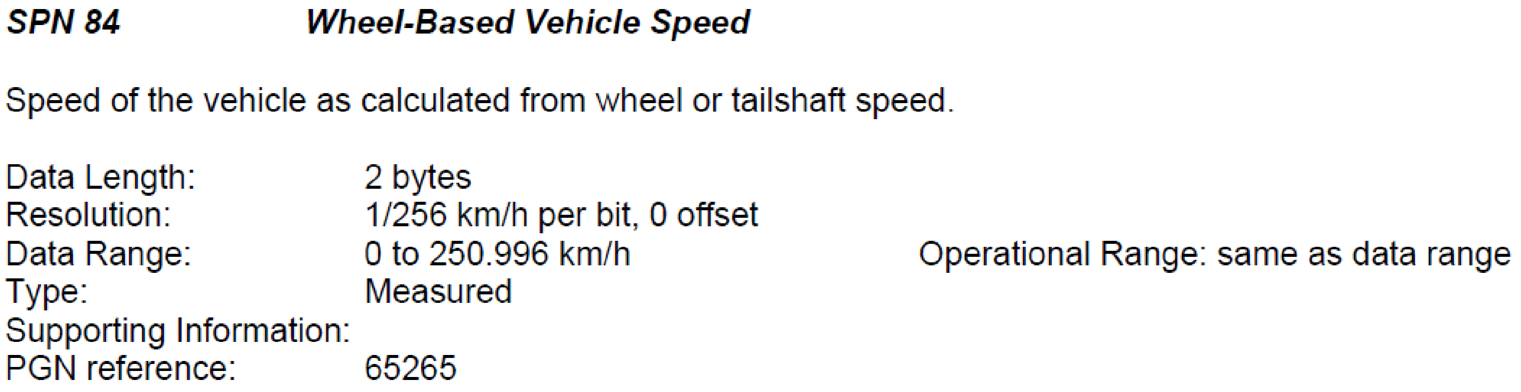


Record 1

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 into data format using J-1939-71



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

- Convert 150 mph to km/h: 241.4 km/h
- Convert 241.4 km/h to bit:

  241.4 km/h x 256 bit/km/h = 64798.4 bit
- Convert 64798.4 to Hex: F1 66
- Look for repeating F1 66 pattern in the FLASH memory

NO PATTERN! WHAT NOW?!

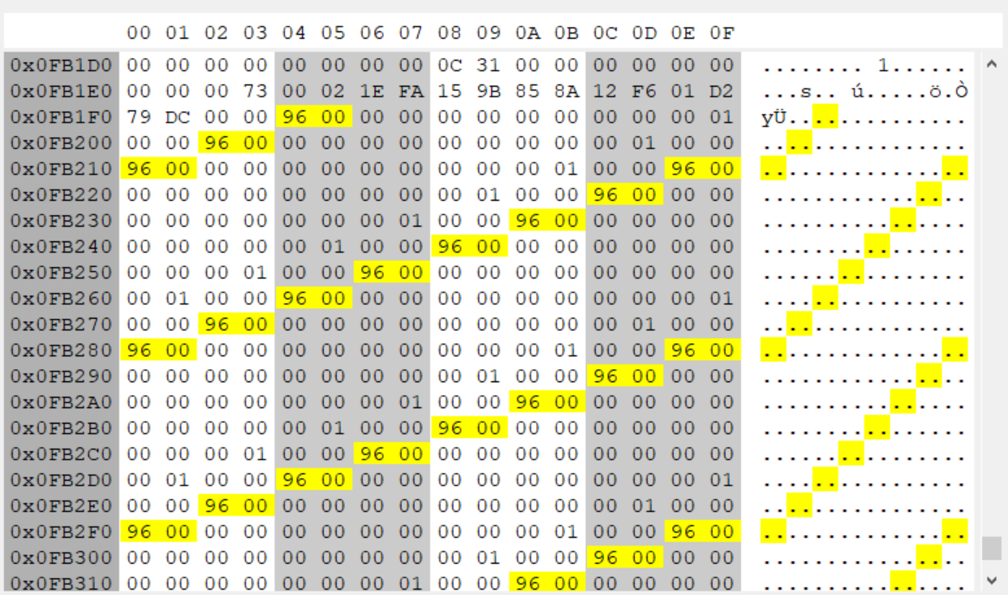
Data Analysis

- Convert 150 mph to data format without converting to km/h
- Convert 150 to bit:

  150 *256 = 38,400
- Convert 38,400 to Hex: 96 00

Data Analysis

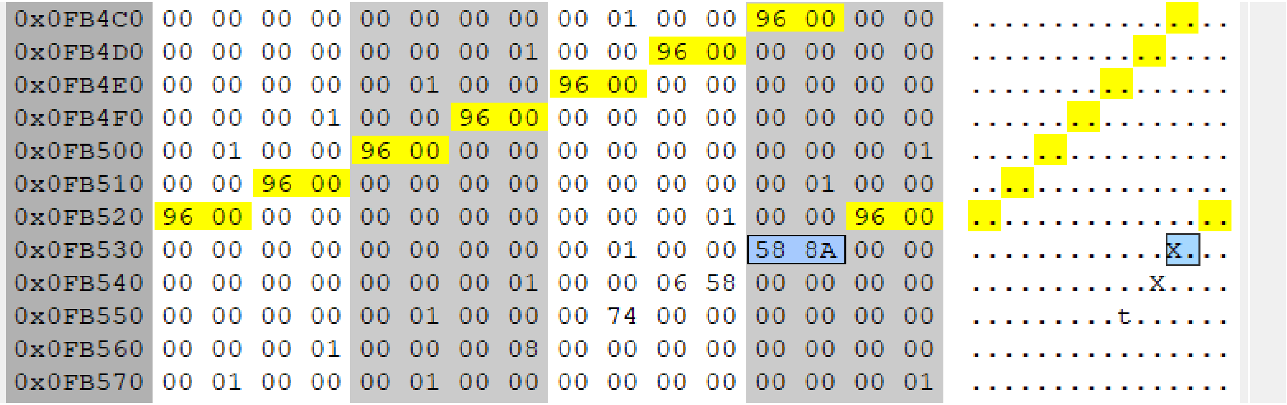
- WOOHOO! We got something



```
            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



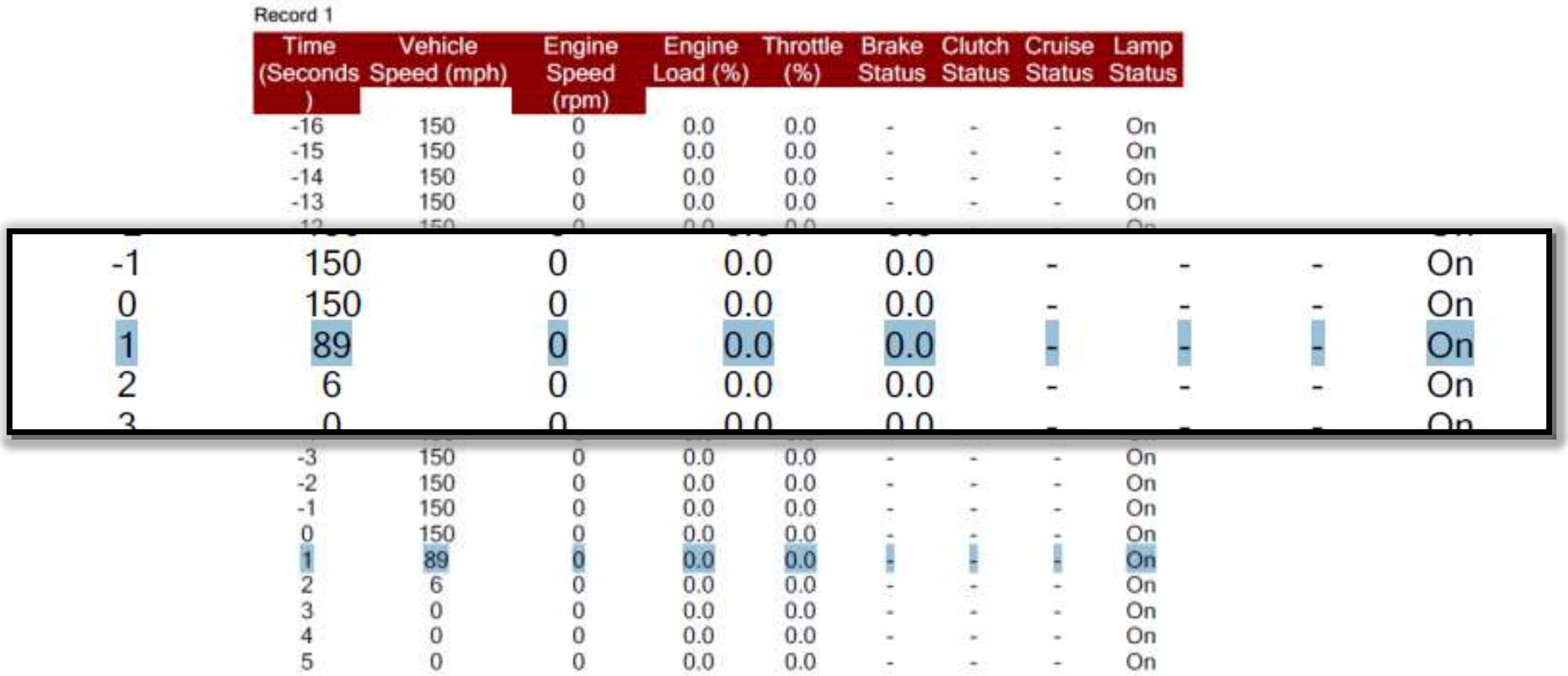
```
0x0FB4C0 00 00 00 00 00 00 00 00 00 01 00 00 96 00 00 00  ................
0x0FB4D0 00 00 00 00 00 00 00 01 00 00 96 00 00 00 00 00  ................
0x0FB4E0 00 00 00 00 00 01 00 00 96 00 00 00 00 00 00 00  ................
0x0FB4F0 00 00 00 01 00 00 96 00 00 00 00 00 00 00 00 00  ................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

Data Analysis

- 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 mph

Data Analysis



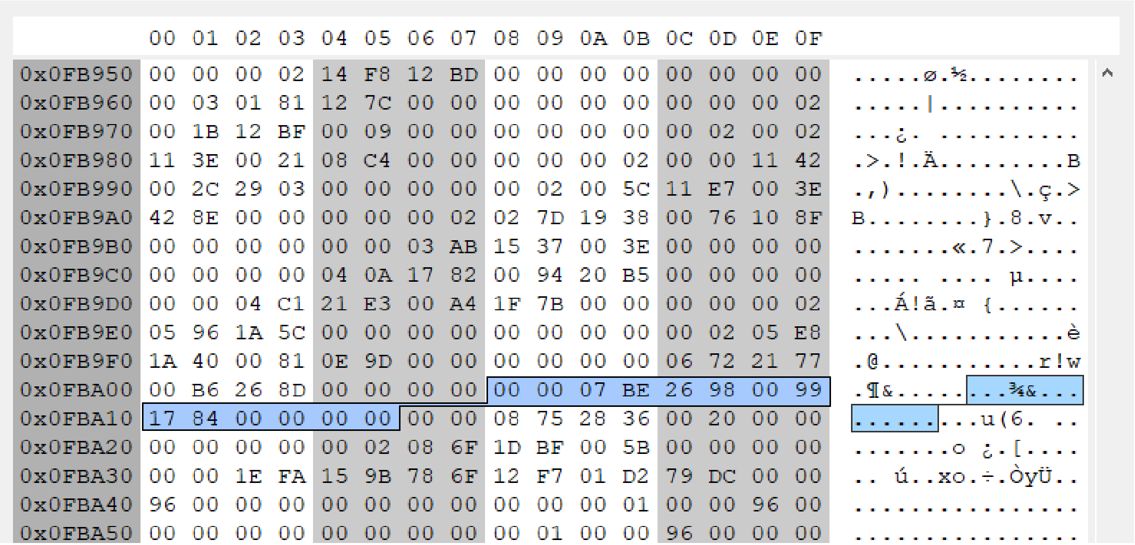
Record 1

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
-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
3	0	0	0.0	0.0	-	-	-	On
4	0	0	0.0	0.0	-	-	-	On
5	0	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
3	0	0	0.0	0.0	-	-	-	On

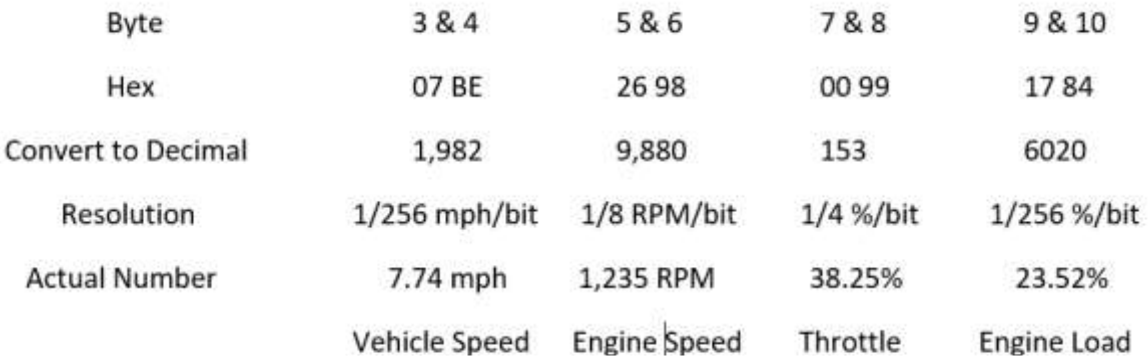
Data Analysis

- What about engine RPM, load, throttle, etc.?
- Take a look at 14-byte block in Record 2 data

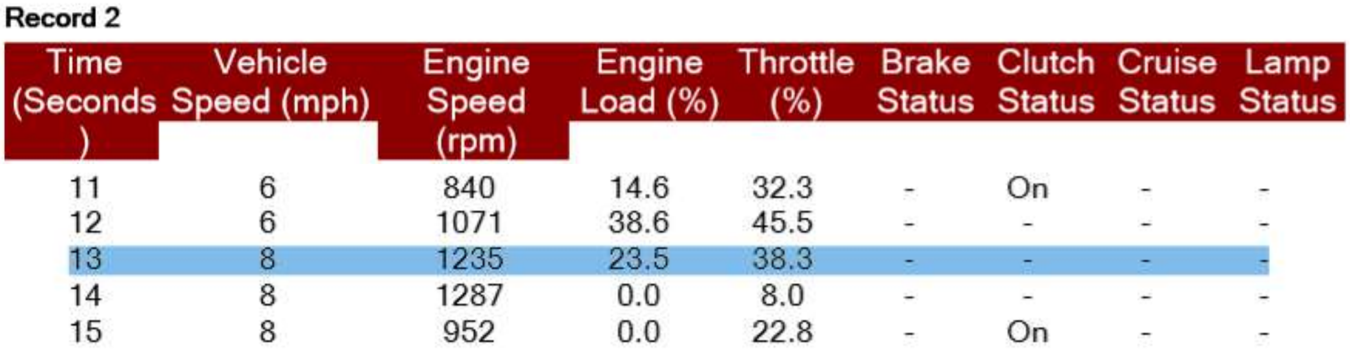


```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0x0FB950  00 00 00 02 14 F8 12 BD 00 00 00 00 00 00 00 00  .....ø.½........
0x0FB960  00 03 01 81 12 7C 00 00 00 00 00 00 00 00 00 02  .....|..........
0x0FB970  00 1B 12 BF 00 09 00 00 00 00 00 00 00 02 00 02  ...¿. ..........
0x0FB980  11 3E 00 21 08 C4 00 00 00 00 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 00  ..... .... µ....
0x0FB9D0  00 00 04 C1 21 E3 00 A4 1F 7B 00 00 00 00 00 02  ...Á!ã.¤ {......
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 00  .........u(6. ..
0x0FBA20  00 00 00 00 00 02 08 6F 1D BF 00 5B 00 00 00 00  .......o ¿.[....
0x0FBA30  00 00 1E FA 15 9B 78 6F 12 F7 01 D2 79 DC 00 00  .. ú..xo.÷.ÒyÜ..
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



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

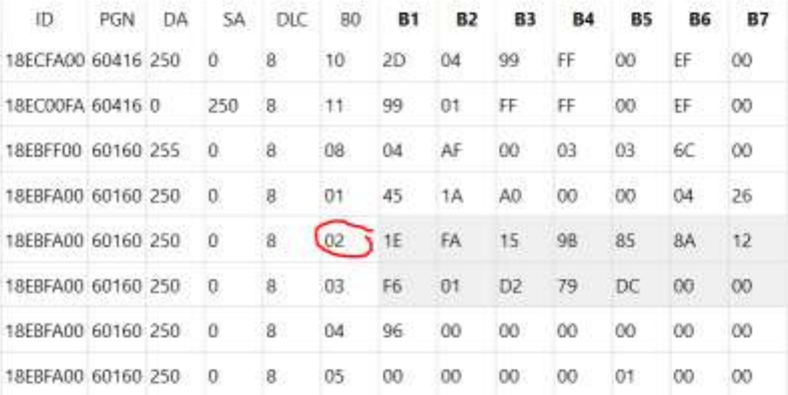


Record 2

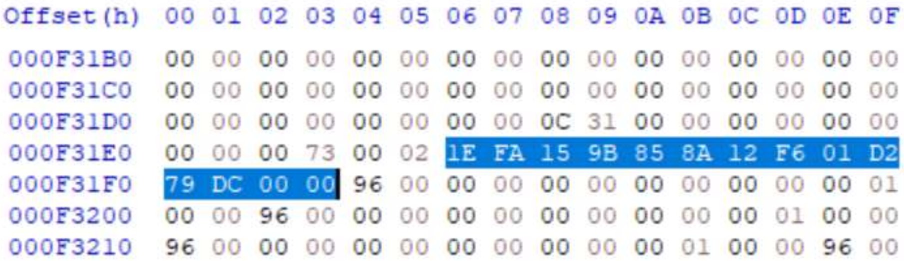
Time (Seconds)	Vehicle Speed (mph)	Engine Speed (rpm)	Engine Load (%)	Throttle (%)	Brake Status	Clutch Status	Cruise Status	Lamp Status
11	6	840	14.6	32.3	-	On	-	-
12	6	1071	38.6	45.5	-	-	-	-
13	8	1235	23.5	38.3	-	-	-	-
14	8	1287	0.0	8.0	-	-	-	-
15	8	952	0.0	22.8	-	On	-	-

Data Analysis

- Comparing memory data with CAN traffic from PowerSpec



ID	PGN	DA	SA	DLC	B0	B1	B2	B3	B4	B5	B6	B7
18ECFA00	60416	250	0	8	10	2D	04	99	FF	00	EF	00
18EC00FA	60416	0	250	8	11	99	01	FF	FF	00	EF	00
18EBFF00	60160	255	0	8	08	04	AF	00	03	03	6C	00
18EBFA00	60160	250	0	8	01	45	1A	A0	00	00	04	26
18EBFA00	60160	250	0	8	02	1E	FA	15	9B	85	8A	12
18EBFA00	60160	250	0	8	03	F6	01	D2	79	DC	00	00
18EBFA00	60160	250	0	8	04	96	00	00	00	00	00	00
18EBFA00	60160	250	0	8	05	00	00	00	00	01	00	00



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

000F31B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000F31C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000F31D0  00 00 00 00 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 12 F6 01 D2
000F31F0  79 DC 00 00 96 00 00 00 00 00 00 00 00 00 00 01
000F3200  00 00 96 00 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 00 00 96 00
```

CAN Traffic from PowerSpec

FLASH Memory

- The results show CAN traffic delivers the exact data from the memory with 7 bytes for every package

Next Steps

- Write a script to parse through raw data to obtain sudden deceleration information
- Explore the specific pattern to find the location of sudden decel for different ECUs
- Write a Hexinator Grammar to automatically analyze binary data
- Correlate network traffic with memory contents
- Publish SAE papers
- Maybe: patch memory to subvert normal functions

Additional Goals

- Analyze multiple ECMs
- Recover data from wrecked ECMs
- Recover data without setting fault codes
- Virtual Chip Swap
- Deep Dive: Build our own KTAG tool

Thank you!

Conclusions

- Three ways of collecting data
  - CAN Data Loggers
    - Version 1 produced over 4000 hours
    - Version 2 has more tool-like features
  - RP1210 Application Logging
    - Fuzzing and Requesting
    - Eavesdropping
  - Memory Interrogation
- Data Analysis
  - Counts and timing
  - Standards based meaning
  - Pattern matching